IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, Plaintiff, v. CHICAGO POLICE DEPARTMENT, CITY OF CHICAGO Defendants.	)	No. 18 CH 07758 Hon. Anna Demacopoulos

NOTICE OF FILING

TO: See Attached Certificate of Service

PLEASE TAKE NOTICE that on **February 1, 2019,** the undersigned caused to be filed with the Clerk of the Circuit Court of Cook County, Illinois, **Plaintiff's Reply In Support of Its Motion for Summary Judgment and Response to Defendants' Cross-Motion,** copies of which are attached and served upon you.

Date: February 1, 2019

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS

By: /s/ Louis A. Klapp
One of Its Attorneys

Karen Sheley
Rachel Murphy
ROGER BALDWIN FOUNDATION OF ACLU, INC.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601
Tel: 312-201-9740
Fax: 312-201-9760
ksheley@aclu-il.org
rmurphy@aclu-il.org

Louis A. Klapp
QUARLES & BRADY LLP
300 North LaSalle Street, Suite 4000
Chicago, IL 60654
Tel: 312-715-5000
Fax: 312-632-1948
louis.klapp@quarles.com

CERTIFICATE OF SERVICE

I, Louis A. Klapp, an attorney, hereby certify that I caused a true and correct copy of the foregoing **Notice of Filing** and **Plaintiff's Reply in Support of Its Motion for Summary Judgment and Response to Defendants' Cross-Motion** referenced therein, to be served upon the following:

AMBER ACHILLES RITTER, Chief Assistant Corporation Counsel
TIA MATHEW, Assistant Corporation Counsel
Legal Information, Investigations, and Prosecutions Division
30 North LaSalle Street, Suite 1720
Chicago, Illinois 60602
tia.mathew@cityofchicago.org
amber.ritter@cityofchicago.org

via e-mail to the addresses indicated and via U.S. Mail, proper first-class postage prepaid, sent on this 1st day of February, 2019, on or before 5:00 p.m.

/s/ Louis A. Klapp
Louis A. Klapp

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, Plaintiff, v. CHICAGO POLICE DEPARTMENT, CITY OF CHICAGO Defendants.	)	No. 18 CH 07758 Hon. Anna Demacopoulos

PLAINTIFF'S REPLY IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT AND RESPONSE TO DEFENDANTS' CROSS-MOTION

I. INTRODUCTION

The City of Chicago is contracting with a private company to spy on the social media accounts of Chicagoans. The City fears that if the public knows the name of the company, the company will be criticized or denied access to private data by other companies (e.g., Facebook or Twitter). Rather than engaging in public debate to justify the contracts, the City has redacted the company's name from the relevant invoices (the "Public Funds Documents"). The Freedom of Information Act ("FOIA") offers no exemptions that justify the redactions. The City spends hundreds of thousands of dollars each year on this social media monitoring software ("SMMS"). Without the company name, the public cannot assess anything about the program: whether it is intrusive, whether it is effective, how it works, and even whether city employees have conflicts of interest when spending public dollars.

Defendants may redact or deny documents only when clear and convincing evidence establishes each any every element of an applicable exemption. Here, Defendants have not met their burden for a simple reason: the information sought by the ACLU is not covered by any exemption. Consistent with the Illinois Constitution, the Public Funds Documents are open for

inspection without condition. Regardless, the elements of Defendants' cited exemptions are not met, as demonstrated by Defendants' lack of evidence. For example, the "specialized investigative technique" exemption applies only if Defendants prove that the alleged technique is not "generally used or known." Defendants outright ignore this element and other elements, providing no evidence to justify the redactions.

Equally flawed is Defendants' attempt to hide the Open Source Records in dispute, which include names of individuals monitored by SMMS. SMMS assesses people's speech; this raises concerns that the software will illegally or unconstitutionally target political opponents or be used in a discriminatory manner. Defendants must meet a fact-intensive standard to withhold the names of their targets, yet Defendants present no evidence whatsoever—not a single sentence in their affidavit—about the nature of the individuals redacted from the Open Source Records. As a matter of law, the documents must be un-redacted.

II. ARGUMENT

A. Unredacted Public Funds Documents Must Be Produced

The Public-Funds Documents—attached as Exhibit 2—are plainly "records relating to the obligation, receipt, and use of public funds," 5 ILCS 140/2.5, which ends the inquiry because such records are not subject to exemption. (*See* Pl. Mem. at 5–6.)[1] As explained below, Defendants' contrary argument breaks basic rules of statutory construction. Regardless, even if Defendants' cited exemptions are available for Section 2.5 documents, the Public-Funds Documents at issue here do not satisfy the exemptions because neither applies to company names on an invoice.

[1] "Pl. Mem." refers to Plaintiff's Memorandum in Support of Its Motion for Summary Judgment. "Defs. Mem." refers to Defendants' Cross Motion for Summary Judgment and Response to Plaintiff's Motion for Summary Judgment. "Romer Aff.," "Gilbert Aff.," and "Massoglia Aff." refer to the Affidavits of Christopher Romer, Dr. Eric Gilbert, and Daniel Massoglia, respectively, filed herewith. "Ex. __" refers to the corresponding exhibit filed herewith. "CPD Aff." refers to the Affidavit of Aaron Cunningham filed with Defendants' Cross Motion.

1. The Public Funds Documents are Section 2.5 records and are not subject to the Section 7 exemptions

In compliance with the Illinois Constitution, the FOIA allows the public to inspect "***[a]ll records*** relating to the obligation, receipt, and use of public funds," and it makes no allowance for redactions or other withholdings. 5 ILCS 140/2.5 (emphasis added) (the "Public-Funds Provision").[2] The Section 7 exemptions simply do not apply to the Public-Funds Documents.

Section 1.2 of the FOIA creates a ***general*** presumption that all records are open for inspection, subject to exemptions if applicable, with Section 7 listing the exemptions. 5 ILCS 140/1.2, 7. However, other provisions make ***specific*** commands about the availability of particular types of documents, including those in Sections 2.5–2.20. These specific sections, to the extent exemptions are contemplated, either explicitly enumerate the exemptions or incorporate those of Section 7 by reference. *E.g.,* 5 ILCS 140/2.10 (listing material that may be redacted), 2.20 (referencing Section 7). Tellingly, the Public-Funds Provision does neither. Thus, no exemptions apply to Public-Funds documents, and they must be disclosed without redactions.

Defendants' reading—that the Section 7 exemptions apply to all provisions, including the Public-Funds Provision—is nonsensical and runs afoul of the canons of statutory interpretation.[3] Under the rule against surplusage, courts have a duty to "give effect, where possible to every word of a statute" *Duncan v. Walker*, 533 U.S. 167, 167 (2001). Therefore, a court "must not read a

---

[2] *See also* Ill. Const., art. VIII § 1(c) ("Reports and records of the obligation, receipt and use of public funds of the State, units of local government and school districts are public records available for inspection by the public according to law.").

[3] Defendants' cite *Kopchar v.City of Chicago* for the proposition that a document fitting within one of the specifically enumerated statutory exemptions is absolutely exempt from disclosure. (Defs. Mem. at 5.) This does nothing to counter the ACLU's argument, as the point is that the relevant documents do not fit within an exemption. Further, Defendants' case was decided before the specific FOIA provisions (*e.g.*, 5 ILCS 140/2.5–2.20) were added to the FOIA, thus they shed no light on the statutory construction dispute here. *Compare* 5 ILCS 140 (Dec. 31, 2009) *with* 5 ILCS 140/2.5 (eff. Jan 1, 2010) (adding § 2.5 per Public Act 96-542).

statute so as to render any part inoperative, superfluous, or insignificant" or to read exceptions the court did not express. *People v. Walker*, 2018 IL App (4th) 170877, ¶ 16. Under Defendants' position, every provision that explicitly refers to Section 7 exemptions would have precisely the same scope if that phrase were eliminated. Defendants' reading renders this language useless. Defendants' position violates the rule against surplusage, so it should be rejected.

2. Defendants have not met—and cannot meet—their burden of showing the applicability of the "unique or specialized investigative techniques" exemption to the Public Funds Documents

Even if exemptions apply to Public Funds Documents, Defendants have not met their burden of proving any exemption. Defendants rely on Section 7(1)(d)(v), which has numerous elements, yet—as shown below—Defendants' purported evidence for each is either nonexistent, conclusory, or easily contradicted.

a. Defendants failed to establish that the Public Funds Documents are records created "for law enforcement purposes"

The Section 7(1)(d)(v) exemption applies only to records "in the possession of . . . any law enforcement or correctional agency ***for law enforcement purposes***." 5 ILCS 140/7(1)(d)(v) (emphasis added). The Public-Funds Documents are invoices. (*See* Ex. 2; Romer Aff. ¶ 3.) By definition, these documents were created to memorialize a procurement transaction, not for any law enforcement purpose. As Defendants state, the Public-Funds Documents were created "to determine and pay companies for software." (Defs. Mem. at 5.)

Defendants ignore this element of the exemption (*id*. at 5–7), as does their declarant (CPD Aff. ¶¶ 1–12). Defendants overreach in claiming that just because the documents memorialize a transaction on behalf of CPD, the documents meet this exemption. That interpretation improperly renders the second half of the relevant statutory language redundant: "Records in the possession of . . . any law enforcement or correctional agency ***for law enforcement purposes***," 5 ILCS

140/7(1)(d) (emphasis added). *See Walker*, 2018 IL App (4th) 170877, ¶ 16. If the General Assembly wanted this exemption to cover all applicable records in the possession of a law enforcement agency, there would have been no need to include the "for law enforcement purposes" language. Yet they did, meaning that ***administrative*** documents are outside the scope of this exemption. This alone is sufficient to deny the exemption.

b. Defendants failed to establish that they seek to withhold a "technique" from public oversight, let alone a "specialized investigative technique"

Defendants also make no attempt to prove that the redaction covers "unique or specialized investigative techniques." 5 ILCS 140/7(1)(d)(v). In particular, they provide no facts (or even argument) concerning whether the thing they seek to withhold from public oversight actually qualifies as a "technique," let alone a "specialized investigative technique."[4] Instead they admit that the redactions hide ***company names***, not techniques, and then parrot the statutory language, thereby assuming away the point they have the burden to prove:

> ***Company names*** are present in the invoices. Based on my knowledge, disclosing the company name reveals the ***specialized investigative techniques and tools*** used by CPD to detect crime and prevent future crime and terrorism.

(CPD Aff. ¶ 5 (emphasis added).)

A company name cannot disclose a technique, and Defendants fail to offer facts to the contrary. (*See* CPD Aff. ¶¶ 1–12.) A company name is useful to the public. It allows an assessment of whether the company was selected because of familial or political connections, or if it has engaged in bad practices in other jurisdictions. Nor is there any basis to conclude that, if a company name is revealed, something that could fairly be called a "technique" would be revealed. A

[4] Defendants reveal (for the first time) that the redacted information in the Public Funds Documents are "company names." (CPD Aff. ¶ 5.)

"technique" is a method of accomplishing a desired aim.[5] Defendants offer no evidence that the present dispute involves a technique, let alone a specialized investigative technique. Consider an unrelated procedure that Defendants would presumably label an "investigative technique": questioning a suspect while measuring certain levels of his blood pressure, pulse, and respiration, and determining whether the suspect's answer to a question is truthful based on a greater than 10% change in the value of either parameter (i.e., a form of polygraph test). If Defendants sought to redact such language from a document, they could explain that the redacted language described the specifics of how the police monitor a person's body to determine truthfulness during an interrogation, a ***factual*** description sufficient to evaluate whether it qualifies as an "investigative technique." Defendants provide no such factual description here. Instead, they just parrot the statutory phrase, "specialized investigative technique." (*E.g.*, CPD Aff. ¶¶ 5, 7.)[6]

Nothing else in the affidavit even purports to justify Defendants' conclusion that the company name reveals an investigative technique. The Court is told only that the product sold by the company is "used by CPD . . . to obtain salient information to be used by detectives and investigators in their criminal investigations, [etc.]"; "led to the identification of criminals"; and "able to enhance public safety." (CPD Aff. ¶¶ 5–7.) That is meaningless, as the same could be alleged about nearly everything the police do. For example, CPD employs patrol officers, who CPD undoubtedly has used to obtain salient information for detectives, identify criminals, and enhance public safety; but that does not make patrol a specialized investigative technique. By turning every police activity into alleged specialized investigative technique, Defendants remove

[5] http://www.merriam-webster.com/dictionary/technique

[6] Defendants apparently recognize that the alleged "specialized investigative technique" may not even be a "technique." Defendants' affiant appears to conflate a "technique" with a "tool." (E.g., CPD Aff. ¶¶ 7–8.) To the extent Defendants are trying to wedge a tool into the Section 7(1)(d)(v) exemption, this is improper: the statute provides no exemption for "tools." 5 ILCS 140/7.

all meaning from the words "specialized" and "investigative." Thus, Defendants offer nothing more than an assertion parroting the language of the statue.

Such conclusory evidence is forbidden by the Supreme Court. Defendants bear the burden of establishing the claimed exemptions with facts—not conclusory assertions. *Day v. City of Chicago*, 388 Ill. App. 3d 70, 75–76 (2009). Invoking the statutory language is insufficient:

> ***[I]n meeting its burden, the public body may not simply treat the words "attorney-client privilege" or "legal advice'" as some talisman, the mere utterance of which magically casts a spell of secrecy over the documents at issu***e. Rather, the public body can meet its burden only by providing some objective indicia that the exemption is applicable under the circumstances.

Illinois Educ. Ass'n v. Illinois State Bd. of Educ., 204 Ill. 2d 456, 470 (2003) (emphasis added); *accord Day*, 388 Ill. App. 3d at 76.

Day addressed whether the City could withhold CPD documents related to an investigation—the one that resulted in the arrest and conviction of the document requestor, Mr. Day—under FOIA's "ongoing criminal investigation exemption," specifically considering whether the City established that the investigation was "ongoing." *Day*, 388 Ill. App. 3d at 74. The City submitted the affidavits of three CPD employees, each of whom claimed the investigation was still ongoing in one form or another. *Id*. at 75–76. For example, one affiant stated that "the investigation is still ongoing, as to certain aspects of the investigation other than Mr. Day's arrest and conviction." *Id*. The other declarations addressed the issue at a similar level of generality. *See id*. at 75–76. Reversing the circuit court, *Day* held that the City failed to meet its burden because it merely "use[d] the term 'ongoing criminal investigation' in its affidavits as some sort of magic talisman," which was plainly deficient in view of Supreme Court precedent. *Id*. (citing *Illinois Education Ass'n*, 204 Ill.2d at 470).

Just as the defendants in *Illinois Education Association* and *Day* tried to repeat the statutory language of "attorney-client privilege" and "ongoing criminal investigation," respectively,

Defendants here do the same thing for "specialized investigative techniques." And just as those cases rejected these as failed magic talismans, this Court should do the same.

Finally, beyond Defendants' failure of proof, the facts show that SMMS does not provide "specialized investigative techniques." SMMS is widely used outside of law enforcement. (Gilbert Aff. ¶¶ 5, 8.) For example, it is employed by marketing and financial professionals. (*Id*.) The mere fact that police may also use SMMS does not convert the functionality of this general-purpose software into "specialized investigative techniques."

c. Defendants failed to establish that the supposed technique is not "generally used and known"

Defendants outright ignore the statutory prohibition against applying the exemption to techniques that are "generally used and known." The brief is silent on the issue. (*See* Defs. Mem. at 5–7.) More fundamentally, the CPD Affidavit—the only evidence put forth by Defendants to meet their burden—alleges nothing whatsoever regarding the extent to which the alleged techniques are used and known. (*See* CPD Aff. ¶¶ 1–12.) That should end it, as there are no facts in the record to support this prong and, thus, the Section 7(1)(d)(v) exemption.

Plus, Defendants have implicitly admitted that the alleged "technique" is well established: Defendants say that mere knowledge of the company name would reveal the alleged technique. (Defs. Mem. at 5.) If that's the case, the alleged technique must necessarily be widely known.[7]

But to the extent there is any doubt, the specific SMMS products on the market are generally used and known. For example, public reporting on police use of SMMS has identified numerous vendors and products by name, including the following: PATHAR, Dunami, TransVoyant, Databricks, Dataminr, and Geofeedia. (Ex. 9 at 1-2; Romer Aff. ¶ 8; *see also* Gilbert

[7] By analogy, if disclosing that a party paid Adobe Inc. would reveal that the party used Photoshop or specific features of that software, such software and features plainly cannot be a secret.

Aff. ¶¶ 9–12.) To state the obvious, companies cannot market and sell their products if they are kept secret, so this information is readily available and not treated as sensitive information. (*See* Gilbert Aff. ¶¶ 9–12.) As another example, Mr. Raimond Ranne, who identifies himself as a former "Analyst/Police Officer" for the City of Chicago, listed the following SMMS products on his publically-available profile: "Lexisnexis, Tweetdeck, Pathar/Dunami, Vigilant/LEARN, CANVAS, . . . Accurint, [and] Genetec." (Ex. 10 at 1; Romer Aff. ¶ 9.)

Indeed, the identity of several specific SMMS products ***used by CPD*** is public knowledge. Publically-available documents show that CPD has employed at least (i) Geofeedia, (ii) Social Media Monitor, and (iii) Dunami. (*E.g.*, Exs. 5–8; Romer Aff. ¶¶ 5–7; Massoglia Aff. ¶ 5.) Consequently, the names of SMMS vendors and their products are generally used and known and, thus, outside the scope of the FOIA exemption.

d. Defendants failed to establish that disclosure of the supposed technique would harm Defendants

Defendants assert an extremely troubling and constitutionally dubious position on the "harm" factor. Defendants contend that, if the public learns on what, and to whom, Defendants spend hundreds of thousands of public dollars annually, the public would become upset and demand change. In particular, they allege that (i) when the public previously learned of CPD's use of Geofeedia, the public outcry resulted in social media platforms disabling Geofeedia's access and (ii) a similar public reaction "discredit[ing] the tool" will lead to the same result for the SMMS product(s) with which CPD replaced Geofeedia. (*See* CPD Aff. ¶¶ 8–10.)

By way of background, Geofeedia—"a CIA-backed social-media monitoring platform that drew fire for enabling law enforcement surveillance"—shifted its business to non-police applications after Twitter, Facebook, and Instagram "cut[] Geofeedia off from [their] valuable data stream[s]." (Ex. 11 at 1-2; Romer Aff. ¶ 10.) Sadly, CPD responded to the public outcry over its

secret use of Geofeedia by hiding its subsequent conduct rather than engaging in a public debate over the value of using and spending so much money on SMMS products. (*See* Ex. 12 at 2 (noting CPD lacked records related to "meeting agendas or minutes, public notice, analyses, communications between law enforcement and elected leaders, or other public process related to the acquisition of [SMMS]"); Romer Aff ¶ 11.)

Defendants' "harm" argument is supported by neither law nor fact. ***First***, the idea that the public may object to CPD's purchase or use of a particular SMMS product is not a "harm to the agency" under the exemption. Defendants' position—that secrecy is justified because Defendants know better than the taxpaying public—is at odds with fundamental democratic principles and the FOIA's stated purpose of encouraging informed debate and oversight:

> [A]ll persons are entitled to full and complete information regarding the affairs of government . . . consistent with the terms of this Act. ***Such access is necessary to enable the people to fulfill their duties of discussing public issues fully and freely, making informed political judgments and monitoring government to ensure that it is being conducted in the public interest***.

5 ILCS 140/1 (emphasis added). Thus, Defendants' reading of the "harm" element is easily rejected as inconsistent with the intent of the statute. *See In re Jarquan B.*, 2017 IL 121483, ¶ 22 ("[t]he cardinal rule in construing a statute is to ascertain and give effect to the legislative intent"); *Prazen v. Shoop*, 2013 IL 115035, ¶ 21 ("in determining the legislative intent of a statute, a court may consider not only the language used, but also the reason and necessity for the law, the evils sought to be remedied, and the purposes to be achieved").

Second, Defendants' alleged consequence is not a harm, but a boon. Aligning CPD's priorities regarding the purchase and use of SMMS with the desires of the public is a good thing. *See* Ill. Const., art. I § 1 (governments derive their just powers "from the consent of the governed").

Third, even assuming Defendants' "harm" argument is a proper application of the FOIA exemption, the facts disprove Defendants' speculation. The idea that public awareness of an

SMMS product will result in its discontinuation conflicts with Defendants' prior use of Social Media Monitor and Dunami. Both products' use by Defendants has been known publically for years, yet Defendants tellingly allege no involuntary cessation of those products.

Defendants' use of Social Media Monitor (by Lexis Nexis) has been publically known since at least November 18, 2016. For example, invoices released by CPD showed that CPD used it since late 2015. (Ex. 8 at 1; Romer Aff. ¶ 7.) Despite this public knowledge, Defendants point to no supposedly harmful ramifications, undoubtedly because there were none. (*See* CPD Aff. ¶¶ 1-12.)

Similarly, Defendants' use of Dunami (by Pathar) has been publically known since at least November 18, 2016. For example, CPD released documents showing its use of Dunami. (Ex. 6 at 1; Romer Aff. ¶ 5.) Two months later, CPD released to a third party an unredacted invoice—apparently identical to one at issue here (except the redactions)—showing CPD's purchase of Dunami. (Massoglia Decl. ¶¶ 3, 5; Ex. 5 at 1; *see* Ex. 2 at 2-5.) That invoice was published on the internet shortly thereafter, and it has been available to the public at large ever since. (*Id*. ¶ 6.) Again, despite the public's knowledge of CPD's purchase and use of Dunami, Defendants cannot identify any supposedly harmful ramifications (because none occurred). (*See* CPD Aff. ¶¶ 1-12.)

Thus, the alleged "harm" cited by Defendants is not a harm as contemplated by the statute and, even if it is, Defendants' speculation about the "harm" is contradicted by their own experiences with Social Media Monitor and Dunami.

3. Defendants have not met—and cannot meet—their burden of showing the applicability of the "vulnerability assessment" exemption to the public-funds documents

Although Defendants also assert the "vulnerability assessment" exemption, they provide no facts to support it. The "vulnerability assessment" exemption concerns certain ***special-purpose*** documents that memorialize the government's assessment of its communities' vulnerabilities to

terrorism-type attacks and the procedures it will take to prevent or respond to such attacks:

> Vulnerability assessments, security measures, and response policies or plans that are ***designed to*** ***identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations***, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community.

5 ILCS 140/7(1)(v) (emphasis added).[8] As its legislative sponsor explained, the "vulnerability assessment" exemption concerned emergency planning documents, not invoices for software:

> [I]t amends the Open Meetings Act and FOIA to allow public bodies to hold closed meetings when considering homeland security issues, ***exempts documents prepared for emergency and security procedures*** from [sic] homeland security where that would be compromised.

(Ex. 13 at 2 (May 31, 2003, Transcript of House of Representatives re HB 954) (emphasis added); *see also* Ex. 14 at 13 (House Bill 954 from 93d General Assembly adding "vulnerability assessment" exemption to the FOIA); Romer Aff. ¶¶ 12-13.)

The "vulnerability assessment" exemption is plainly inapplicable here. Indeed, the CPD Aff. does not even utter the phrases "vulnerability assessments," "security measures," or "response policies or plans." (*See* CPD Aff. ¶¶ 1–12.) Likewise, it does not claim that Public Funds Documents disclose the areas of the city that Defendants have deemed vulnerable "to potential attacks upon [the] community's population or systems, facilities, or installations" or the plans Defendants have in place to prevent or respond to such attacks. (*Id*.)

Having no evidence on point, Defendants simply adopt their argument for the "specialized investigative technique" exemption. (Defs. Mem. at 7.) For example, they state that public

[8] *See also* 49 C.F.R. § 1520.3 (defining "vulnerability assessment"); *Schreibman v. U.S. Dep't of Commerce*, 785 F. Supp. 164, 165 (D.D.C. 1991) (agreeing that the following documents, characterized by government's witness as "classic 'vulnerability assessments,'" could be withheld under Federal FOIA: "records [that] note problems with the computer security plans and contain advice and recommendations on measures that can be taken to insure the security of the computer systems.").

displeasure may result in the elimination of a "tool [used] to combat terrorism and investigate crime" if the associated company name is disclosed. (*Id.*) As explained previously, this speculation is inapplicable and disproven by Defendants' own history with SMMS. (*See* Section II.A.2.d.)

Regardless, Defendants' entire argument is irrelevant and misses the point. Even if the alleged "tool" (sometimes characterized by Defendants as a "tool/technique") is one of the devices in Defendants' arsenal for investigating crime and combatting terrorism, that does not convert invoices for the "tool" into vulnerability assessments or other special document type "designed to" perform the functions covered by Section 7(1)(v). That exemption is limited to documents disclosing Defendants' assessment of the city's vulnerability to a terrorism-type attack or describing how Defendants will prevent or respond to such an attack. Invoices showing who, and how much, Defendants paid for a "tool" used for general police purposes are inapplicable.

B. Unredacted Open Source Records Must Be Produced

As stated in the Complaint, the use of SMMS that principally concerns the ACLU in this matter is the monitoring of citizens merely because they are engaged in activity protected by the First Amendment, such as protesting the inauguration of President Trump. (Complaint ¶¶ 2–7.)

Defendants do not state whether any individual identified in the Open Source Records were monitored because of social media posts referencing protests or movements (*e.g.*, Black Lives Matter). Since the beginning of this litigation, the ACLU has sought information on whether such records are in dispute here, including by requesting an index of redacted documents to better understand the nature of the withheld information. (*See* Sept. 27, 2018, Order.) However, at every turn—including in Defendants' briefing—Defendants used only the vaguest descriptions of the persons identified in the Open Source Records.

Nonetheless, the ACLU has endeavored to identify the most important Open Source Records, and it narrows its request to the documents compiled in Exhibit 3 (the "Disputed OSRs").

As explained below, Defendants have not met their burden of withholding the names of individuals in these records under the Section 7(1)(c) "personal information" exemption.

1. Defendants present no evidence about the individuals identified in the Disputed OSRs

Defendants present no evidence related to the Open Source Records, so Defendants necessarily have not met their burden. Determining whether a disclosure would constitute an unwarranted invasion of personal privacy is a ***fact-intensive inquiry*** that considers the following factors: "(1) the plaintiff's interest in disclosure, (2) the public interest in disclosure, (3) the degree of invasion of personal privacy, and (4) the availability of alternative means of obtaining the requested information." *Nat'l Ass'n of Criminal Def. Lawyers v. Chicago Police Dep't*, 399 Ill. App. 3d 1, 13 (2010). Yet, The CPD Affidavit—Defendants' only evidence—is completely silent on all issues related to the Open Source Records (including the Disputed OSRs), so Defendants necessarily have not met their burden. For example, while Defendants state that "[m]ost of the redactions made to the records were identifying information of victims," that is pure attorney argument. (*See* Defs. Mem. at 9.)

2. Defendants unsupported generalities are insufficient to redact names from the Disputed OSRs

Even if the attorney argument could be deemed evidence—it cannot—Defendants' argument is woefully deficient. "To meet [their] burden and to assist the court in making its determination, the agency must provide a *detailed* justification for its claimed exemption, ***addressing the requested documents specifically*** and in a manner allowing for adequate adversary testing." *Illinois Education Ass'n*, 204 Ill.2d at 464 (italics in original; bold-italics added). Without providing a factual justification for redacting each ***specific*** Disputed OSR (either individually or by grouping Disputed OSRs with similar information), Defendants cannot justify the exemption and allow for adversary testing. *See id*. Consider the redaction in this Disputed OSR:

011TH DISTRICT- JA494452@1300HRS-600 S KOSTNER

[redacted] NO IR#

NEGATIVE RESULTS AT THIS TIME

(Ex. 3 at 9) Assuming the name of an individual is beneath the redaction, it is impossible to tell whether he or she was monitored by CPD because, for example, he was a victim of a crime or was a person with no connection to a crime, but strong connection to the Black Lives Matter movement. The public's interest in knowing whether a protest leader was illicitly monitored is obviously much greater than knowing the identity of a victim. Yet, Defendants' failure to provide any evidence—let alone sufficient evidence—about this document demonstrates the inability to apply the four-factor test and, thus, Defendants' failure of proof. Thus, the exemption does not apply.

III. CONCLUSION

For these reasons, summary judgment should be granted in the ACLU's favor and against Defendants. The Public Funds Documents (Ex. 2) must be un-redacted in full and the Disputed OSRs (Ex. 3) must be un-redacted to show the identity of the monitored citizens.

Date: February 1, 2019

Respectfully submitted,

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS

By: /s/ Louis A. Klapp
One of Its Attorneys

Karen Sheley
Rachel Murphy
ROGER BALDWIN FOUNDATION OF ACLU, INC.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601
Tel: 312-201-9740
Fax: 312-201-9760
ksheley@aclu-il.org
rmurphy@aclu-il.org

Louis A. Klapp
QUARLES & BRADY LLP
300 North LaSalle Street, Suite 4000
Chicago, IL 60654
Tel: 312-715-5000
Fax: 312-632-1948
louis.klapp@quarles.com

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, Plaintiff, v. CHICAGO POLICE DEPARTMENT, CITY OF CHICAGO Defendants.	)	No. 18 CH 07758 Hon. Anna Demacopoulos

AFFIDAVIT OF CHRISTOPHER ROMER

I, Christopher Romer, do solemnly affirm and certify, under the penalties provided under Section 1-109 of the Illinois Code of Civil Procedure, that if called as a witness, I would testify that the following facts are true and correct to the best of my knowledge and belief and are based on my personal knowledge:

1. I am a legal assistant at the ACLU of Illinois ("ACLU"). In that capacity, I have knowledge of the documents sent or received pursuant to the ACLU's October 19, 2016, and January 2, 2018, requests to the Chicago Police Department ("CPD") under the Freedom of Information Act ("FOIA") and during this litigation.

2. The document designated Exhibit 1 is a true and correct copy of a letter the ACLU received in response to its January 2, 2018, FOIA request.

3. The document designated Exhibit 2 is a compilation of true and correct copies of excerpts from the document production sent to the ACLU from CPD in response to the ACLU's January 2, 2018, FOIA request.

4. The document designated Exhibit 3 is a compilation of true and correct copies of excerpts from the document production sent to the ACLU from CPD in response to the ACLU's January 2, 2018, FOIA request.

5. The document designated Exhibit 6 is a true and correct excerpt from the document production sent to the ACLU from CPD in response to the ACLU's October 19, 2016, FOIA request.

6. The document designated Exhibit 7 is a true and correct excerpt from the document production sent to the ACLU from CPD in response to the ACLU's October 19, 2016, FOIA request.

7. The document designated Exhibit 8 is a true and correct excerpt from the document production sent to the ACLU from CPD in response to the ACLU's October 19, 2016, FOIA request.

8. The document designated Exhibit 9 is a true and correct copy of an article titled, "No Surprise: CIA Reportedly Funds Companies That Can Spy On You Via Twitter And Instagram" and dated April 16, 2016, which was printed from the following URL: https://www.techtimes.com/articles/150780/20160416/no-surprise-cia-reportedly-funds-companies-that-can-spy-on-you-via-twitter-and-instagram.htm.

9. The document designated Exhibit 10 is a true and correct copy of a LinkedIn profile printed on September 28, 2017, from the following URL: https://www.linkedin.com/in/raimondranne/.

10. The document designated Exhibit 11 is a true and correct copy of an article titled, "Geofeedia cuts half of staff after losing access to Twitter, Facebook" and dated November 21, 2016, which was printed from the following URL: https://www.chicagotribune.com/bluesky/originals/ct-geofeedia-cuts-jobs-surveillance-bsi-20161121-story.html.

11. The document designated Exhibit 12 is a true and correct copy of the letter the ACLU received in response to its October 19, 2016, FOIA request.

12. The document designated Exhibit 13 is a true and correct copy of excerpts from the May 31, 2003, Transcription of Debate from the Illinois House of Representatives, which was downloaded from the following URL: http://www.ilga.gov/house/transcripts/htrans93/09300069.pdf.

13. The document designated Exhibit 14 is a true and correct copy of HB0954 from the 93rd Illinois General Assembly, which was downloaded from the following URL: http://www.ilga.gov/legislation/93/HB/PDF/09300HB0954lv.pdf.

14. The document designated Exhibit 15 is a true and correct copy of an article titled, "Everything you need to know about the Cambridge Analytica-Facebook debacle" and dated March 20, 2018, which was printed from the following URL: https://www.chicagotribune.com/bluesky/technology/ct-biz-cambridge-analytica-facebook-20180320-story.html.

15. The document designated Exhibit 16 is a true and correct copy of an article titled, "Reddit Limits Noxious Content by Giving Trolls Fewer Places to Gather" and dated September 25, 2017, which was printed from the following URL: https://www.nytimes.com/2017/09/25/business/reddit-limits-noxious-content-by-giving-trolls-fewer-places-to-gather.html.

16. The document designated Exhibit 17 is a true and correct copy of a webpage printed from the following URL: https://www.dataminr.com/press/article-dataminr-announces-new-tool-to-assist-first-responders.

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and

correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be true.

FURTHER AFFIANT SAYETH NOT

By: 
Christopher Romer

Date: 2/1/19

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, Plaintiff, v. CHICAGO POLICE DEPARTMENT, CITY OF CHICAGO Defendants.	)	No. 18 CH 07758 Hon. Anna Demacopoulos

AFFIDAVIT OF DR. ERIC GILBERT

I, Eric Gilbert, do solemnly affirm and certify, under the penalties provided under Section 1-109 of the Illinois Code of Civil Procedure, that if called as a witness, I would testify that the following facts are true and correct to the best of my knowledge and belief and are based on my personal knowledge:

1. I am the John Derby Evans Associate Professor in the School of Information at the University of Michigan in Ann Arbor, Michigan, a post that I have held since 2017. From 2011 through 2017, I was an Assistant Professor in the College of Computing, Georgia Institute of Technology in Atlanta, Georgia. In 2010, I received my PhD from the University of Illinois at Urbana-Champaign in Computer Science. In 2001, I received my BS from the University of Illinois at Urbana-Champaign, where I majored in Mathematics and Computer Science.

2. My research focuses on building and studying social media systems.

3. I understand that the American Civil Liberties Union of Illinois ("ACLU") sought records from the Chicago Police Department ("CPD") regarding CPD's purchase and use of "social media monitoring software," which the ACLU defined to mean "an application that

enables the monitoring, searching, collection, or analysis of user-generated content located on social media services" such as Facebook, Instagram, Twitter.

4. Most social medial platforms (e.g., Facebook, Instagram, Twitter) sell, or otherwise make available, their users' social media posts and information about those posts ("social media data").

5. Many software companies sell social media monitoring software that allows their clients (e.g., corporations, political candidates, governmental entities) to access and use the social media data made available by social medial platforms. For example, as reflected on its website (dataminr.com), Dataminr markets its social media monitoring software for the following applications: public relations and communications, journalists, finance, and first responders.

6. Companies that sell social media monitoring software typically gain access to social media data from the major social media platforms via an application programming interface ("API") developed by each platform. An API is a type of software designed to facilitate communication between two different applications (in this case, social media platforms and social media monitoring software). Each social media platform's API allows any approved person or entity to get access to the platform's data (or a subset of data), typically in exchange for a fee for non-academic applications.

7. I use social media data in my research. For example, in one study we accessed a large volume of Twitter data through Twitter's API and used it to determine whether trolls (i.e., users masquerading as someone different than their true identity) could be identified as such based on their behavioral signals. As another example, we accessed a large volume of Reddit

data through Reddit's API and studied whether the steps taken by Reddit to enforce its ban of certain hate groups were effective.

8. Companies use social media data for a variety of reasons. For example, marketing and public relations professionals use the data to understand how their brand is being discussed and the effectiveness of their marketing campaigns. As another example, finance professionals (i.e., hedge funds) use social media monitoring software to quickly detect events and identify trading opportunities generated by those events.

9. The monitoring of social media data is well publicized. For example, much was written about Cambridge Analytica's access and use of large quantities of Facebook data during the 2016 presidential election, including in the document labeled Exhibit 15. Indeed, even academic studies that involve collecting and using social media data, such as my own work, are frequently reported on by the press. For example, the work regarding Reddit's hate-group ban mentioned above was discussed in a New York Times article titled, "Reddit Limits Noxious Content by Giving Trolls Fewer Places to Gather," on September 25, 2017, which is shown in the document labeled Exhibit 16. The article discussed our research, including by noting that "[t]he researchers analyzed 100 million posts originating on two forums on Reddit."

10. In my experience, companies that make and sell social media monitoring software are publically known. For example, social media monitoring companies such as Dataminr and Palantir are attendees at conferences directed to social media monitoring. As another example, most of these companies maintain webpages promoting their software (e.g., dataminr.com, palantir.com).

11. Use of social media monitoring software by government entities is also publically known. For example, the document labeled Exhibit 9, contains a discussion of PATHAR

(Dunami), TransVoyant, Databricks, Dataminr, and Geofeedia in an April 16, 2016, article. As another example, as reflected on its website (palantir.com), Palantir explicitly markets its social media monitoring software to law enforcement, and includes case studies of its use by police in Salt Lake City and Los Angeles.

12. Similarly, in my experience, the companies that make and sell social media monitoring software promote various features and functionality of their software. For example, as reflected on their website, in May 2017, "Dataminr introduced a new product on stage at TechCrunch Disrupt in New York City that searches the Twitter firehose for emergency situations throughout the city, and channels news alerts to first responders" (see Exhibit 17). As another example, Plantir's webpage directed to law enforcement—palantir.com/solutions/law-enforcement—notes that its software allows police offers to "conduct geo-searches around locations of interest and view relevant arrest data, calls for service, and notes and photos from previous investigations."

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be true.

FURTHER AFFIANT SAYETH NOT

By: 

Dr. Eric Gilbert

Date: _____

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, Plaintiff, v. CHICAGO POLICE DEPARTMENT, CITY OF CHICAGO Defendants.	)	No. 18 CH 07758 Hon. Anna Demacopoulos

AFFIDAVIT OF DANIEL MASSOGLIA

I, Daniel Massoglia, do solemnly affirm and certify, under the penalties provided under Section 1-109 of the Illinois Code of Civil Procedure, that if called as a witness, I would testify that the following facts are true and correct to the best of my knowledge and belief and are based on my personal knowledge:

1. I am over the age of 18 and if called to testify would be competent to do so.

2. I am a resident of the City of Chicago.

3. On Saturday, December 31, 2016, I submitted a request under the Freedom of Information Act ("FOIA") to the Chicago Police Department (at foia@chicagopolice.org) for the following records:

> Please produce all records related to expenditures by the Chicago Police Department and/or the City of Chicago for the purchase or license of any social media surveillance or monitoring software, hardware, or services, including but not limited to those provided by the firm Geofeedia. This request can be understood to include records related to the acquisition of "predictive policing" tools.

4. The document labeled Exhibit 4 is a true and correct copy of the letter I received in response to my FOIA request.

5. The document labeled Exhibit 5 is one of the records sent to me in response to my FOIA request.

6. On or about January 17, 2017, I posted the document labeled Exhibit 5 to github.com, a website that allows open sharing of documents and information. The document has been continuously available to the public from on or about January 17, 2017, through today at the following address: https://github.com/jujueyeball/social-media-monitoring.

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

FURTHER AFFIANT SAYETH NOT

By: _____
Daniel Massoglia

Subscriber and sworn to me on this 29th day of January, 2019.

_____

MARIANA KARAMPELAS
OFFICIAL SEAL
Notary Public, State of Illinois
My Commission Expires
September 07, 2021

EXHIBIT 1

DEPARTMENT OF LAW
CITY OF CHICAGO

August 17, 2018

Louis A. Klapp
louis.klapp@quarles.com

Re: **American Civil Liberties Union of Illinois, 18 CH 07758**

Dear Mr. Klapp:

In an attempt to resolve matters in connection with the above-identified lawsuit, the City is providing you with records in response to the Freedom of Information Act ("FOIA") request you submitted. In your request dated January 2, 2018, you sought the following records:

> *The ACLU of Illinois requests the following records:*
>
> 1. *All contracts related to the purchase, acquisition, installation, maintenance, or use of social media monitoring software.*
> 2. *All invoices related to social media monitoring software.*
> 3. *All manuals, guides, training materials, or other instructional records related to social media monitoring software.*
> 4. *All policies governing access, use, or training related to social media monitoring software.*
> 5. *All directives governing access, use, or training related to social media monitoring software.*
> 6. *All Open Source receipts (or other reports of usage) related to the use of social media monitoring software by the CPD Crime Prevention and Information Center since October 2, 2017.*

In response to item 1, please find attached responsive contracts.

In response to item 2, CPD has attached responsive invoices. Signatures were redacted pursuant to Section 7(1)(b) of FOIA. Section 7(1)(b) exempts from disclosure, "[p]rivate information, unless disclosure is required by another provision of this Act, a State or federal law or a court order." 5 ILCS 140/7(1)(b). "Private information" is defined in section 2(c-5) as "unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email

addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person." 5 ILCS 140/2(c-5). Therefore, signatures were properly redacted.

CPD also made redactions to a specialized investigative tool. Section 7(1)(d)(v) exempts records that would, "[d]isclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request." Release of that redaction would reveal a unique and specialized technique/tool used by CPD, where disclosure would render it ineffective and harm CPD's ability to use an effective crime fighting tool and therefore is exempt pursuant to Section 7(1)(d)(v).

Moreover, this technique/ tool/ measure is exempt pursuant to Section 7(1)(v). 5 ILCS 140/7(1)(v) provides that "[v]ulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations." Release of that redaction would reveal a unique and specialized technique/tool/measure used by CPD, where disclosure of the technique/ tool/ measure would render it ineffective and therefore is exempt pursuant to Section 7(1)(v).

In response to item 3, CPD asked individuals in its Crime Prevention Information Center (CPIC) whether they had guides or training materials related to social media monitoring software. While they did receive training, individuals in CPIC did not locate any records responsive to this portion of the request.

In response to item 4 and item 5, please find enclosed responsive policies and directives.

In response to item 6, CPD has provided responsive Open Source records. Please be advised that names, IR numbers, instagram addresses, icons, screennames, photos, twitter names and account information, snapchat information, school information, employment information, and facebook numbers and usernames, and other identifying information of individuals found in these reports were redacted pursuant to Section 7(1)(c) of FOIA. Section 7(1)(c) exempts, "[p]ersonal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information." 5 ILCS 140/7(1)(c) Because the redacted information is personal information and individuals would find it objectionable for the public to know that the CPD was reviewing their social media accounts, release would be an invasion of personal privacy. Therefore, CPD properly redacted this information pursuant to Section 7(1)(c).

If you have any remaining concerns about your FOIA request, please contact me.

Please let me know if we can resolve this matter and discuss settlement.

Sincerely,

Tia Mathew
Assistant Corporation Counsel
312-744-1052

EXHIBIT 2

57

System Solutions Inc.

3630 Commercial Ave. DEPT. A
Northbrook IL 60062
(847) 272-6160

RECEIPT # 588153 INVOICE

INVOICE # : 457639
DATE : 11/13/2014

	SOLD	SHIP
Name	CITY OF CHICAGO-CPD	CITY OF CHICAGO-CPD-UNIT 125
Address	1411 W. MADISON ST., ATTN:DANIEL HODGES - A/P CHICAGO, IL 60607 312-746-9205	3510 S. MICHIGAN ATTN:DANIEL HODGES 13783-8433 CHICAGO, IL 60653

P.O. #	SHIP DATE	SHIP VIA	F.O.B	TERMS	SOLDBY
13783-8433	11/13/2014	DROP SHIP	NORTHBROOK	NET 30	DH

Qty	Sqty	B/O	Part #	Description	Unit	Total
4	4		[redacted]	[redacted] SEAT LIC WITH DATA PLAN NAMED USER LIC WITH FOR EMPLOYEE DATA FEES TO ACCESS HISTORICAL DATA TERM: 5 MONTHS 9/5/14 to 2/8/15.	16500.00	66000.00

PVCI14CI028454

SUBTOTAL		66,000.00
TAX	GOVERNMENT	
TOTAL		66,000.00

NOTICE : ACCOUNTS PASTDUE WILL BE ASSESSED A SERVICE CHARGE OF 1.5% PER MONTH.
ALL SALES ARE FINAL. ONLY DEFECTIVE ITEMS WILL BE EXCHANGED AND REPLACE WITH IDENTICAL MERCHANDISE (OR REPLACE ON SOME ITEMS) WITHIN 5 DAYS OF PURCHASE DATE.
TITLE OF EQUIPMENTS WILL REMAIN WITH System Solutions Inc. UNTILL ABOVE INVOICE IS FULLY PAID
* items are non taxable

109581 Customer Signature _____ Print Name _____ Date/Time _____

Ex. 2-1

System Solutions Inc.

58

3630 Commercial Ave. DEPT. A
Northbrook IL 60062
(847) 272-6160

PVCI14CI006171

RECEIPT # 555959

INVOICE

INVOICE # 452448
DATE 03/28/2014

	SOLD	SHIP
Name	CITY OF CHICAGO-CPD	CITY OF CHICAGO-CPD
Address	1411 W. MADISON ST.,	1411 W. MADISON ST.,
	ATTN:DANIEL HODGES - A/P	ATTN:DANIEL HODGES 13783-7990
	CHICAGO, IL 60607	CHICAGO, IL 60607
	312-746-9205	

P.O. #	SHIP DATE	SHIP VIA	F.O.B	TERMS	SOLDBY
13783-7990	03/28/2014	DROP SHIP	NORTHBROOK	NET 30	DH

Qty	Sqty	B/O	Part #	Description	Unit	Total
1	1		CTC [redacted]	[redacted] 120 DAY ONSITE SUPPORT TO INCLUDE THE FOLLOWING: QTY 4 [redacted] SEAT LICENSES/DATA PLANS QTY 4 3-DAY SOCIAL MEDIA COURSE CHICAGO GANG MAPPING/ANALYTICS 4/1/2014 TO 9/30/14 Asset Tag # A001036 Per Dan Hodges (CPD)	216000.00	216000.00

RECEIVED
MAY 20 2014
CITY COMPTROLLERS OFFICE

SUBTOTAL		216,000.00
TAX	GOVERNMENT	
TOTAL		216,000.00

NOTICE : ACCOUNTS PAST DUE WILL BE ASSESSED A SERVICE CHARGE OF 1.5% PER MONTH.
ALL SALES ARE FINAL, ONLY DEFECTIVE ITEMS WILL BE EXCHANGED AND REPLACE WITH IDENTICAL MERCHANDISE (OR REPLACE ON SOME ITEMS) WITHIN 5 DAYS OF PURCHASE DATE.
TITLE OF EQUIPMENTS WILL REMAIN WITH System Solutions Inc. UNTILL ABOVE INVOICE IS FULLY PAID
* Items are non taxable

105000 Customer Signature _____ Print Name _____ Date/Time _____

Ex. 2-2

FY15 5A

[redacted] REMIT PAYMENT TO: [redacted]

INVOICE

ACH INFORMATION:
THE NORTHERN TRUST
50 SOUTH LASALLE STREET
CHICAGO, IL 60675

E-mail Remittance To: gschremittance@cdw.com
ROUTING NO.: 071000152
ACCOUNT NAME: CDW GOVERNMENT
ACCOUNT NO.: 91057

CDW Government
75 Remittance Drive, Suite 1515
Chicago, IL 60675-1515

RETURN SERVICE REQUESTED

PVCI15CI009984

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
TT04487	04/13/15	9760892
SUBTOTAL	SHIPPING	SALES TAX
$270,900.00	$0.00	$0.00
DUE DATE		AMOUNT DUE
06/12/15		$270,900.00

618800
7.17

CITY OF CHICAGO- DOIT
DEPARTMENT OF FINANCE
50 W WASHINGTON ST RM 2700
CHICAGO IL 60602-7300
USA

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

PLEASE RETURN THIS PORTION WITH YOUR PAYMENT

INVOICE DATE	INVOICE NUMBER	PAYMENT TERMS	DUE DATE
04/13/15	TT04487	Net 60 Days	06/12/15
ORDER DATE	SHIP VIA	PURCHASE ORDER NUMBER	CUSTOMER NUMBER
04/03/15	ELECTRONIC DISTRIBUTION	29669-273	9760892

ITEM NUMBER	DESCRIPTION	QTY ORD	QTY SHIP	QTY B/O	UNIT PRICE	TOTAL
3629717	[redacted] [redacted] CONC LIC Manufacturer Part Number: [redacted] Term 2/9/15-12/31/15 Electronic distribution - NO MEDIA Cost Center:057-125 POLICE Asset Tag: A001036 CPD DAN HODGES UNIT 125 [redacted] [redacted] LIC	1	1	0	270,900.00	270,900.00

OK to Pay
7.20

RECEIVED
JUL 20 2015
City of Chicago Finance Dept.

GO GREEN!
CDW is happy to announce that paperless billing is now available! If you would like to start receiving your invoices as an emailed PDF, please email CDW at paperlessbilling@cdw.com. Please include your Customer number or an Invoice number in your email for faster processing.

REDUCE PROCESSING COSTS AND ELIMINATE THE HASSLE OF PAPER CHECKS!
Begin transmitting your payments electronically via ACH using CDW's bank and remittance information located at the top of the attached payment coupon. Email credit@cdw.com with any questions.

ACCOUNT MANAGER	SHIPPING ADDRESS:	SUBTOTAL	$270,900.00
JENNIFER LAGONI 312-705-9093 jennandmeagan@cdwg.com	CITY OF CHICAGO- POLICE ATTN:DANIEL HODGES 3510 S MICHIGAN CHICAGO IL 60653	SHIPPING	$0.00
		SALES TAX	$0.00
SALES ORDER NUMBER		AMOUNT DUE	$270,900.00
1BJRWZ2			

Cage Code Number 1KH72
DUNS Number 02-615-7235

ISO 9001 and ISO 14001 Certified
CDW GOVERNMENT FEIN 36-4230110

HAVE QUESTIONS ABOUT YOUR ACCOUNT?
PLEASE EMAIL US AT credit@cdw.com
VISIT US ON THE INTERNET AT www.cdwg.com

James, Michele

From: CDW <cdwsales@cdwemail.com>
Sent: Tuesday, August 02, 2016 11:45 AM
To: CDWG Account Team - Jen and Meagan
Subject: CDW-G Invoice #CMR6797 Detail

REMIT PAYMENT TO:
CDW Government
75 Remittance Drive Suite 1515
Chicago, IL 60675-1515

THE CDW-G INVOICE #CMR6797 YOU REQUESTED IS DETAILED BELOW

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
CMR6797	03/24/2016	9760892
SUBTOTAL	SHIPPING	SALES TAX
$74,468.00	$0.00	$0.00
DUE DATE		AMOUNT DUE
05/23/2016		$74,468.00

ORDER DATE	SHIP VIA	ORDER #	PO #	PAYMENT TERMS
03/21/2016	ELECTRONIC DISTRIBUTION	1BMMV0D	29659-931	Net 60 Days

ITEM	ORDER QTY	SHIP QTY	OPEN QTY	CDW#	UNIT PRICE	EXT. PRICE
[redacted] ONG LIC Mfg. Part#: [redacted] **Contract:** **CITY OF CHICAGO HARDWARE SOFTW** **29659-105081** January 1 2016-April 4 2016 Electronic distribution - NO MEDIA Four Concurent user licenses for up to twelve name users Data fees to access histrocial social media data	1	1	0	3629717	$74,468.00	$74,468.00

IMPORTANT - PLEASE READ

Additional Information:

Cost Center: 057 CPD

PURCHASER BILLING INFO	DELIVER TO		
Billing Address: CITY OF CHICAGO-"DOIT" DEPARTMENT OF FINANCE 333 S STATE ST LOWR LL30 CHICAGO, IL 60604-3947	**Shipping Address:** CITY OF CHICAGO- CPD ATTN:DANIEL HODGES 3510 S MICHIGAN CHICAGO, IL 60653	**Subtotal:**	$74,468.00
		Shipping:	$0.00
		Sales Tax:	$0.00
		AMOUNT DUE:	$74,468.00

2 ways to GO GREEN with CDW-G! Paperless billing and electronic payment transmission

TRANSMIT PAYMENTS ELECTRONICALLY — Eliminate the hassle of paper checks by utilizing ACH for electronic bill pay.
EMAIL REMITTANCE TO: gachremittance@cdw.com

Ex. 2-4

Blustain, Lawrence H.

From: CDW <cdwsales@cdwemail.com>
Sent: Tuesday, October 04, 2016 9:15 AM
To: CDWG Account Team - Jen and Meagan
Subject: CDW-G Invoice #CMH2748 Detail

REMIT PAYMENT TO:
CDW Government
75 Remittance Drive Suite 1515
Chicago, IL 60675-1515

THE CDW-G INVOICE #CMH2748 YOU REQUESTED IS DETAILED BELOW

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
CMH2748	03/23/2016	9760892
SUBTOTAL	**SHIPPING**	**SALES TAX**
$227,932.00	$0.00	$0.00
DUE DATE		**AMOUNT DUE**
05/22/2016		$227,932.00

ORDER DATE	SHIP VIA	ORDER #	PO #	PAYMENT TERMS
03/21/2016	ELECTRONIC DISTRIBUTION	18MMTZ9	29659-929	Net 60 Days

ITEM	ORDER QTY	SHIP QTY	OPEN QTY	CDW#	UNIT PRICE	EXT. PRICE
[redacted] CONC LIC Mfg. Part#: [redacted] Contract: CITY OF CHICAGO HARDWARE SOFTW 29659-105081 04/05/16-12/31/16 to twelve name users Data fees to access historical social media data Electronic distribution - NO MEDIA Four Concurent user licenses for up	1	1	0	3629717	$227,932.00	$227,932.00

IMPORTANT - PLEASE READ

Additional Information:

Cost Center:057 CPD

PURCHASER BILLING INFO

Billing Address:
CITY OF CHICAGO-"DOIT"
DEPARTMENT OF FINANCE
333 S STATE ST LOWR LL30
CHICAGO, IL 60604-3947

DELIVER TO

Shipping Address:
CITY OF CHICAGO- CPD
ATTN:DANIEL HODGES
3510 S MICHIGAN
312-745-5545
CHICAGO, IL 60653

Subtotal:	$227,932.00
Shipping:	$0.00
Sales Tax:	$0.00
AMOUNT DUE:	$227,932.00

2 ways to GO GREEN with CDW-G! Paperless billing and electronic payment transmission

TRANSMIT PAYMENTS ELECTRONICALLY — Eliminate the hassle of paper checks by utilizing ACH for electronic bill pay.

Order# 57055 - 730927

REMIT PAYMENT TO:

INVOICE

ACH INFORMATION:
THE NORTHERN TRUST
50 SOUTH LASALLE STREET
CHICAGO, IL 60675

E-mail Remittance To: gschremittance@cdw.com
ROUTING NO.: 071000152
ACCOUNT NAME: CDW GOVERNMENT
ACCOUNT NO.: 91057

CDW Government
75 Remittance Drive, Suite 1515
Chicago, IL 60675-1515

RETURN SERVICE REQUESTED

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
HVJ5444	05/12/17	9760892
SUBTOTAL	**SHIPPING**	**SALES TAX**
$308,160.00	$0.00	$0.00
DUE DATE		**AMOUNT DUE**
07/11/17		**$308,160.00**

CITY OF CHICAGO- DOIT
DEPARTMENT OF FINANCE
333 S STATE ST LOWR LL30
CHICAGO IL 60604-3947
USA

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

PLEASE RETURN THIS PORTION WITH YOUR PAYMENT

INVOICE DATE	INVOICE NUMBER	PAYMENT TERMS	DUE DATE
05/12/17	HVJ5444	Net 60 Days	07/11/17
ORDER DATE	**SHIP VIA**	**PURCHASE ORDER NUMBER**	**CUSTOMER NUMBER**
04/26/17	ELECTRONIC DISTRIBUTION	57055.0.21	9760892

ITEM NUMBER	DESCRIPTION	QTY ORD	QTY SHIP	QTY B/O	UNIT PRICE	TOTAL
3029717	[redacted] CONC LIC Manufacturer Part Number: [redacted] 01.01.2017 -12.31.2017 Quantity 4 Concurrent [redacted] Analytics Subscription Plus data package. 3 named users max per subscription Electronic distribution - NO MEDIA CPD Unit 122 Financial Services	1	1	0	308,160.00	308,160.00

Received OK
9 June 2017

BASED UPON THE SIGNATURES OF THE
RECEIVING UNIT, THIS INVOICE HAS BEEN
APPROVED FOR PAYMENT.

APPROVED BY: DATE:
7 Jun 17.

GO GREEN!
CDW is happy to announce that paperless billing is now available! If you would like to start receiving your invoices as an emailed PDF, please email CDW at paperlessbilling@cdw.com. Please include your Customer number or an Invoice number in your email for faster processing.

REDUCE PROCESSING COSTS AND ELIMINATE THE HASSLE OF PAPER CHECKS!
Begin transmitting your payments electronically via ACH using CDW's bank and remittance information located at the top of the attached payment coupon. Email credit@cdw.com with any questions.

ACCOUNT MANAGER	SHIPPING ADDRESS:		
JENNIFER LAGONI 312-705-9093 jennandmeagan@cdwg.com	CITY OF CHICAGO- DOIT BROWN, JOEL W 3510 S. MICHIGAN AVE. 3RD FLOOR CHICAGO IL 60653	SUBTOTAL	$308,160.00
		SHIPPING	$0.00
		SALES TAX	$0.00
SALES ORDER NUMBER		**AMOUNT DUE**	$308,160.00
LB38734			

Cage Code Number 1KH72
DUNS Number 02-616-7236

ISO 9001 and ISO 14001 Certified
CDW GOVERNMENT FEIN 36-4230110

HAVE QUESTIONS ABOUT YOUR ACCOUNT?
PLEASE EMAIL US AT credit@cdw.com
VISIT US ON THE INTERNET AT www.cdwg.com

Ex. 2-6

REMIT PAYMENT TO:

INVOICE

ACH INFORMATION:
THE NORTHERN TRUST
50 SOUTH LASALLE STREET
CHICAGO, IL 60675

E-mail Remittance To: pachremittance@cdw.com
ROUTING NO.: 071000152
ACCOUNT NAME: CDW GOVERNMENT
ACCOUNT NO.: 91057

CDW Government
75 Remittance Drive, Suite 1515
Chicago, IL 60675-1515

RETURN SERVICE REQUESTED

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
LLM9445	01/19/18	9760892
SUBTOTAL	**SHIPPING**	**SALES TAX**
$308,160.00	$0.00	$0.00
DUE DATE		**AMOUNT DUE**
03/20/18		**$308,160.00**

CITY OF CHICAGO- DOIT
DEPARTMENT OF FINANCE
333 S STATE ST LOWR LL30
CHICAGO IL 60604-3947
USA

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

PLEASE RETURN THIS PORTION WITH YOUR PAYMENT

INVOICE DATE	INVOICE NUMBER	PAYMENT TERMS				DUE DATE
01/19/18	LLM9445	Net 60 Days				03/20/18
ORDER DATE	**SHIP VIA**	**PURCHASE ORDER NUMBER**				**CUSTOMER NUMBER**
01/18/18	ELECTRONIC DISTRIBUTION	70799:0:21				9760892
ITEM NUMBER	**DESCRIPTION**	**QTY ORD**	**QTY SHIP**	**QTY B/O**	**UNIT PRICE**	**TOTAL**
3629717	[redacted] CONC LIC Manufacturer Part Number: [redacted] 12.31.2017-12.30.2018 12 months Rel 8 subscription, Electronic distribution - NO MEDIA 057-4125 DISTRICT POLICE HEADQUARTER S Quote JMNH833	1	1	0	308,160.00	308,160.00

Agst #
A001036

Ordered
6/19/18

GO GREEN!

CDW is happy to announce that paperless billing is now available! If you would like to start receiving your invoices as an emailed PDF, please email CDW at paperlessbilling@cdw.com Please include your Customer number or an Invoice number in your email for faster processing.

REDUCE PROCESSING COSTS AND ELIMINATE THE HASSLE OF PAPER CHECKS!

Begin transmitting your payments electronically via ACH using CDW's bank and remittance information located at the top of the attached payment coupon. Email credit@cdw.com with any questions.

ACCOUNT MANAGER	SHIPPING ADDRESS:		
JENNIFER LAGONI 312-705-9093 jennandmeagan@cdwg.com	CITY OF CHICAGO- DOIT HODGES, DANIEL J 3510 S. MICHIGAN AVE. CHICAGO IL 60653	SUBTOTAL	$308,160.00
		SHIPPING	$0.00
SALES ORDER NUMBER		SALES TAX	$0.00
NK95390		**AMOUNT DUE**	**$308,160.00**

Cage Code Number 1KH72
DUNS Number 02-515-7235

ISO 9001 and ISO 14001 Certified
CDW GOVERNMENT FEIN 36-4230110

HAVE QUESTIONS ABOUT YOUR ACCOUNT?
PLEASE EMAIL US AT credit@cdw.com
VISIT US ON THE INTERNET AT www.cdwg.com

Ex. 2-7

EXHIBIT 3

JA549380 – 6528 S Green – 009 – S

OSINT OFFICER / ANALYST ASSIGNED: Richardson WATCH: 3rd

DATE OCCUR. / TIME OCCUR. : 14 Dec 17 1809 HRS

[redacted] / IR# [redacted]

INTELLIGENCE DISCOVERED:

No social media account found at this time.

POSITIVE INFORMATION:

JA549522 – 5346 S Talman – 009 – S

OSINT OFFICER / ANALYST ASSIGNED: Richardson WATCH: 3rd

DATE OCCUR. / TIME OCCUR. : 14 Dec 17 2008 Hrs

[redacted] IR# [redacted]

INTELLIGENCE DISCOVERED:

None at this time.

POSITIVE INFORMATION:

RD# JA550938 – Location 826 W Windsor – Dist. 019 Occ. – MVs

OSINT OFFICER / ANALYST ASSIGNED: R. Lopez #17882 WATCH: 1st

DATE OCCUR. / TIME OCCUR. : 15Dec17/2247hrs

VICTIM(S) NAME / IR# [redacted]/No IR

[redacted]/No IR

INTELLIGENCE DISCOVERED: Negative Results

POSITIVE INFORMATION:

JA556938 – 3114 S. Lituanica Ave – 009 – S

OSINT OFFICER / ANALYST ASSIGNED: Richardson WATCH: 3rd

DATE OCCUR. / TIME OCCUR. : 20 Dec 2017

[redacted] / IR#[redacted]

INTELLIGENCE DISCOVERED:

None at this time.

POSITIVE INFORMATION:

None

RD#JA560334 – 7037 S. Carpenter – 007 – S

OSINT OFFICER / ANALYST ASSIGNED:Sullivan WATCH: 2nd

DATE OCCUR. / TIME OCCUR. : 23 Dec 17 0645

[redacted] / IR#[redacted]

INTELLIGENCE DISCOVERED:

Negative results

POSITIVE INFORMATION:

RD# JA565479 – 401 S. Kilpatrick – 011 – H

OSINT OFFICER / ANALYST ASSIGNED: Sullivan WATCH: 2nd

DATE OCCUR. / TIME OCCUR. :1157hrs

[redacted] IR [redacted]

INTELLIGENCE DISCOVERED:

https://www.facebook.com/[redacted]

POSITIVE INFORMATION:

Facebook page found negative results locating any incriminating information

011TH DISTRICT- JA494424@1246HRS-1130 S RICHMOND

[redacted] IR#[redacted]

NEGATIVE RESULTS AT THIS TIME

007TH DISTRICT- JA494435@1308HRS-1035 W 59TH ST

[redacted] IR# [redacted]

NEGATIVE RESULTS AT THIS TIME

011TH DISTRICT- JA494452@1300HRS-600 S KOSTNER

[redacted] NO IR#

NEGATIVE RESULTS AT THIS TIME

011TH DISTRICT JA494564@1421HRS-3340 W CONGRESS PKWY (M)

[redacted] IR#[redacted] 4CH- BODY SNATCHER

NEGATIVE RESULTS AT THIS TIME

010TH DISTRICT JA494615@1520HRS- 1246 S LAWNDALE

[redacted] IR# [redacted] TVL- 13TH AND LAWNDALE

WWW.FACEBOOK.COM/[redacted] PRIVATE ACCOUNT

NO ACTIONABLE DATA AT THIS TIME

009TH DISTRICT JA494969@1905HRS- 4201 S KEDZIE

[redacted] NO IR#

NEGATIVE RESULTS AT THIS TIME

JA498190 – 3919 W. 47th St. – 008 – M

Peabody #15257: 2nd WATCH

04-Nov-2017/ 0344 hrs.

[redacted] / NO IR

INTELLIGENCE DISCOVERED:

Results Negative at this Time

POSITIVE INFORMATION:

DNA

JA498200 – 7434 S. Colfax Ave. – 003 – S

Peabody #15257: 2nd WATCH

04-Nov-2017/ 0330 hrs.

[redacted] / IR# [redacted]

INTELLIGENCE DISCOVERED:

https://www.facebook.com[redacted]

POSITIVE INFORMATION:

DNA

JA498335 – 1320 S. Albany Ave. – 010 – S

Peabody #15257: 2nd WATCH

04-Nov-2017/ 0916 hrs.

[redacted] /IR #[redacted]

INTELLIGENCE DISCOVERED:

Negative Results at this Time

POSITIVE INFORMATION:

DNA

JA499186 – 7976 S. Kolin Ave. – 008 – S

Peabody #15257: 2nd WATCH

04-Nov-2017/ 2137 hrs.

[redacted] /IR #[redacted]

INTELLIGENCE DISCOVERED:

www.facebook.com[redacted] twitter @[redacted]

POSITIVE INFORMATION:

DNA

JA499276 – 5949 S. Campbell Ave. – 008 – S

Peabody #15257: 2nd WATCH

04-Nov-2017/ 2309 hrs.

[redacted] /IR #[redacted]

INTELLIGENCE DISCOVERED:

Negative Results at this Time

POSITIVE INFORMATION:

DNA

JA499322 – 145 E. 117th Pl. – 005 – S (MV)

Peabody #15257: 2nd WATCH

05-Nov-2017/ 0013 hrs.

[redacted]/IR #[redacted]

INTELLIGENCE DISCOVERED:

www.facebook.com/[redacted]

POSITIVE INFORMATION:

DNA

[redacted]/NO IR

INTELLIGENCE DISCOVERED:

Negative Results at this Time

POSITIVE INFORMATION:

DNA

RD# JA-510725 – 4501 W. MADISON – 011 Dist. – SHOOTING

OSINT OFFICER / ANALYST ASSIGNED: MEDICI#3410 WATCH: 3RD

UPDATE BY OSINT OFFICER/ANALYST :LOPEZ#17882 WATCH:1ST

13NOV17/1848 HRS.

[redacted] IR#[redacted]

INTELLIGENCE DISCOVERED:

NO INTELLIGENCE FOUND.

UPDATE: www.facebook.com/[redacted]

POSITIVE INFORMATION:

NONE FOUND.

EXHIBIT 4

Rahm Emanuel
Mayor

Department of Police • City of Chicago
3510 South Michigan Avenue • Chicago, Illinois 60653

Eddie T. Johnson
Superintendent of Police

January 17, 2017

VIA E-MAIL
Dan Massoglia
dmassoglia@gmail.com

Re: NOTICE OF RESPONSE TO FOIA REQUEST
REQUEST DATE: January 3, 2016
FOIA FILE NO.: P055971

Dear Mr. Massoglia:

The Chicago Police Department (CPD) is in receipt of your Freedom of Information Act (FOIA) request stating:

"Please produce all records related to expenditures by the Chicago Police Department and/or the City of Chicago for the purchases or license of any social media surveillance or monitoring software, hardware, or services, including but not limited to those provided by the firm Geofeedia. This request can be understood to include records related to the acquisition of "predictive policing" tools."

Your request has been reviewed by the undersigned. After consulting with the CPD Finance Division, it has been determined that your request is **granted**. FOIA is releasing the most recent records on file regarding purchases or license of any social media surveillance or monitoring software, hardware, or services, including but not limited to those provided by the firm Geofeedia.

Please be advised that pursuant to 5 ILCS 140/7(1)(b), the FOIA exempts the release of "[p]rivate information, unless disclosure is required by another provision of this Act, a State or federal law or a court order." Private information is defined as:

> U]nique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person. 5 ILCS 140/2(c-5).

Additionally, incident addresses when it is a home address, personal addresses, and any CPD personnel unique identification numbers like employee user code numbers, unique handwritten signatures, and employee numbers contained in these records are private information and have been properly redacted pursuant to Section 7(1)(b).

If I can be of further assistance, you may contact me at (312) 745-5308, or by mail at the following address:

Chicago Police Department
Attn: Freedom of Information Officer
Office of Legal Affairs, Unit 114
3510 S. Michigan Ave.
Chicago, IL 60653

You have a right of review by the Illinois Attorney General's Public Access Counselor (PAC). You can file a request for review by writing to:

Public Access Counselor
Office of the Attorney General
500 S. 2nd Street
Springfield, Illinois 62706
Phone: 312-814-5526 or 1-877-299-FOIA (1-877-299-3642)
Fax: 217-782-1396 E-mail: publicaccess@atg.state.il.us

If you choose to file a Request for Review with the PAC, you must do so within 60 calendar days of the date of a denial letter. 5 ILCS 140-9.5(a). When filing a Request for Review, you must include a copy of the original FOIA request and a denial letter. You may also seek judicial review of a denial under 5 ILCS 140/11 by filing a lawsuit in the State Circuit Court.

Sincerely,

K. Washington

K. Washington, FOIA Officer
Freedom of Information Division
Chicago Police Department
Legal Affairs

EXHIBIT 5

James, Michele

From: CDW <cdwsales@cdwemail.com>
Sent: Tuesday, August 02, 2016 11:45 AM
To: CDWG Account Team - Jen and Meagan
Subject: CDW-G Invoice #CMR6797 Detail

REMIT PAYMENT TO:
CDW Government
75 Remittance Drive Suite 1515
Chicago, IL 60675-1515

THE CDW-G INVOICE #CMR6797 YOU REQUESTED IS DETAILED BELOW

INVOICE NUMBER	INVOICE DATE	CUSTOMER NUMBER
CMR6797	03/24/2016	9760892
SUBTOTAL	**SHIPPING**	**SALES TAX**
$74,468.00	$0.00	$0.00

DUE DATE	AMOUNT DUE
05/23/2016	**$74,468.00**

ORDER DATE	SHIP VIA	ORDER #	PO #	PAYMENT TERMS
03/21/2016	ELECTRONIC DISTRIBUTION	1BMMV0D	29659-931	Net 60 Days

ITEM	ORDER QTY	SHIP QTY	OPEN QTY	CDW#	UNIT PRICE	EXT. PRICE
PATHAR DUNAMI CONC LIC **Mfg. Part#: DUNAMI** **Contract:** **CITY OF CHICAGO HARDWARE SOFTW** **29659-105081** January 1 2016-April 4 2016 Electronic distribution - NO MEDIA Four Concurent user licenses for up to twelve name users Data fees to access histrocial social media data	1	1	0	3629717	$74,468.00	$74,468.00

IMPORTANT - PLEASE READ
Additional Information: Cost Center:057 CPD

PURCHASER BILLING INFO	DELIVER TO		
Billing Address: CITY OF CHICAGO-"DOIT" DEPARTMENT OF FINANCE 333 S STATE ST LOWR LL30 CHICAGO, IL 60604-3947	**Shipping Address:** CITY OF CHICAGO- CPD ATTN:DANIEL HODGES 3510 S MICHIGAN CHICAGO, IL 60653	**Subtotal:**	$74,468.00
		Shipping:	$0.00
		Sales Tax:	$0.00
		AMOUNT DUE:	**$74,468.00**

2 ways to GO GREEN with CDW-G! Paperless billing and electronic payment transmission

TRANSMIT PAYMENTS ELECTRONICALLY – Eliminate the hassle of paper checks by utilizing ACH for electronic bill pay.
EMAIL REMITTANCE TO: gachremittance@cdw.com

ACH INFORMATION: The Northern Trust, 50 South LaSalle St., Chicago, IL 60675

ROUTING NO.: 071000152 | **ACCOUNT NAME:** CDW Government | **ACCOUNT NO.:** 91057

PAPERLESS BILLING NOW AVAILABLE — If you would like to start receiving your invoices as an emailed PDF, please contact us at paperlessbilling@cdw.com. Please include your customer number or an invoice number in your request for faster processing.

SALES CONTACT INFO

JENNIFER LAGONI | (312) 705-9093 | jennandmeagan@cdwg.com

Help and Information: Support | About Us | Privacy Policy | Terms and Conditions

This email was sent to JennandMeagan@cdwg.com.
Please add cdwsales@cdwemail.com to your address book.

AS-1:001 | iSeries 004 | Customer#: 9760892 | EC35F401-183319DC-84460004-AC1BBA2D

Ex. 5-2

EXHIBIT 6

CRIME PREVENTION & INFORMATION CENTER

OPEN SOURCE

OPEN SOURCE INTELLIGENCE GROUP OSIG

OSINT ACTION TO MURDERS AND SHOOTINGS

Date of Incident	25 Oct 16	Time	1900 Hrs	RD#	HZ-488946
Location of Incident	[redacted]			District of Incident	009
Submitting Member Name	Connolly			[redacted]	

[redacted]

List Geofences Created:

[redacted]

List Keywords Searched:

[redacted] shot, shoot, gang

Narrative of Intelligence Discovered: (Include negative and/or new unrelated information)

A preliminary search yielded negative results. Negative dunami results.

Positive Intelligence Notification for follow up made to: (preferably by phone)

Unit	Name/Rank	Star	Date	Time

EXHIBIT 7

PVCI15CI014378

CDW GOVERNMENT, LLC.

Name and address information about this vendor will appear on the city's website at www.cityofchicago.org

City of Chicago
Office of City Comptroller
Room 700
121 N. LaSalle Street
Chicago, IL 60602

Order Payment Voucher

Voucher Number	Voucher Total	Vendor Number – Site Code	Page
PVCI15CI014378	23,100.00	1064105 - A (EFT1057)	1

Remittance Address:
CDW GOVERNMENT, LLC.
75 REMITTANCE DRIVE
CHICAGO, IL 60675-1515

Release Date: 04/03/2015

Delivered To:
006-2005 MAIN OFF
333 S. STATE
ROOM LL30
Chicago-IL

Prepared By : CAROL S.
Approval Date: 07/10/2015

Vendor Inv #: TQ06956 **Type** STANDARD **Date:** 04/03/2015 **PO#** 29659 **Rel#** 274 **Rcv Date:** 07/09/2015

Desktop Computer Software

Ln	Commodity / Description	Qty Recd	Unit of Meas.	Unit Cost	Total Cost
1	20880.28 Desktop Computer Software	23,100.00	USD	1.00	23,100.00

Invoice Number: TQ06956 **Total:** 23,100.00

Grand Total: **23,100.00**

Accounting Information :

Invoice	Ln	BFY	FUND	Cost Ctr	Appr	Accnt	Actv	Project	Rpt Cat	Genrl	Futr	Total Cost
TQ06956	1	014	0N31	0571005	0140	220140	0000	00000000	14MU3M	00000	0000	23,100.00
Grand Total:												**23,100.00**

		Dept Certification of Receipt	Dept Certification of Contract Prices
Entered By		I hereby certify that the invoices have not been previously vouchered and that the goods or services indicated were received and that the account is approved from appropriations as shown above..	I hereby certify that the Department Project Manager has verified the work, services or goods for which payment is sought are as described in the contract and at the price charged in the contract.
Auditor's Approval			
Received By		Authorized Signature / Date	Commissioner or Dept Head / Date

Ex. 7-1

CDW·G

CDWG.com | 800.594.4239 OE400SPS

SALES QUOTATION

QUOTE NO.	ACCOUNT NO.	DATE
FZJB453	9760892	3/5/2015

BILL TO:
CITY OF CHICAGO-"DOIT"
50 W WASHINGTON ST RM 2700

Accounts Payable
CHICAGO , IL 60602-7300

Customer Phone #312.744.4900

SHIP TO:
CITY OF CHICAGO-"DOIT"
Attention To: DEPARTMENT OF FINANCE
50 W WASHINGTON ST RM 2700

CHICAGO , IL 60602-7300
Contact: DANIEL
HODGES 312.746.9205

Customer P.O. # GEOFEEDIA QUOTE

ACCOUNT MANAGER	SHIPPING METHOD	TERMS	EXEMPTION CERTIFICATE
JENNIFER LAGONI 866.339.7925	ELECTRONIC DISTRIBUTION	Net 60-verbal	GOVT-EXEMPT

QTY	ITEM NO.	DESCRIPTION	UNIT PRICE	EXTENDED PRICE
1	3639439	GEEOFEEDIA ENT LIC 1Y 40U Mfg#: COCGEEOFEEDIA Contract: MARKET Term: 12 months, April 2, 2015 - April 1, 2016 Electronic distribution - NO MEDIA	23,100.00	23,100.00
		SUBTOTAL		23,100.00
		FREIGHT		0.00
		TAX		0.00
			US Currency TOTAL	23,100.00

CDW Government
230 North Milwaukee Ave.
Vernon Hills, IL 60061

Fax: 312.705.9193

Please remit payment to:
CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

This quote is subject to CDW's Terms and Conditions of Sales and Service Projects at
http://www.cdwg.com/content/terms-conditions/product-sales.aspx
For more information, contact a CDW account manager.

EXHIBIT 8

PV57155700569

Name and address information about this vendor will appear on the city's website at www.cityofchicago.org

City of Chicago
Office of City Comptroller
Room 700
121 N. LaSalle Street
Chicago, IL 60602

Direct Payment Voucher

LEXISNEXIS BUSINESS&ACADEMIC

Voucher Number	Voucher Total	Vendor Number – Site Code	Page
PV57155700569	6,532.00	50085964 - C	1

Remittance Address:
LEXISNEXIS BUSINESS&ACADEMIC
PO BOX 7247-6157
PHILADELPHIA, PA 191706157

Delivered To:
DEPARTMENT OF POLICE

Prepared By : BULLOCK 5-5642
Approval Date: 12/01/2015

Vendor Invoice Number: 1609131-20151231P **Vendor Invoice Date:** 11/05/2015
SOCIAL MEDIA MONITOR

LN	Commodity /Description	Quantity	Unit Of Meas.	Unit Cost	Total Cost
1	91579-TELECOMMUNICATION SERVICES (NOT OTHERWISE CLASSIFIED)	0	N	0	6,532.00

Vendor Invoice Number: 1609131-20151231P **Total:** 6,532.00

Grand Total: **6,532.00**

Accounting Information :

Invoice	Ln	BFY	FUND	Cost Ctr	Appr	Accnt	Actv	Project	Rpt Cat	Genrl	Futr	Total Cost
1609131-20151231P	1	014	0N31	0571005	0140	220140	0000	00000000	14MU3M	00000	0000	6,532.00

Grand Total: **6,532.00**

		Department Approval	Department Approval
Entered By		I hereby certify that the invoices have not been previously vouchered and that the goods or services indicated were received and that the account is approved from appropriations as shown above.	I hereby certify that the invoices have not been previously vouchered and that the goods or services indicated were received and that the account is approved from appropriations as shown above.
Auditor's Approval		Authorized Signature / Date	Signature / Date
Received By			

Ex. 8-1

EXHIBIT 9

No Surprise: CIA Reportedly Funds Companies That Can Spy On You Via Twitter And Instagram

16 April 2016, 8:49 am EDT By Santiago Tiongco Tech Times

The Central Intelligence Agency (CIA) is reportedly funding companies that spy on Twitter and Instagram feeds to monitor any signs of "unusual activity."

Through its venture capital firm, In-Q-Tel (IQT), the CIA has made investments in "social media mining and surveillance" companies previously undisclosed. These include PATHAR, TransVoyant, Databricks, Dataminr, and Geofeedia.

The information was obtained from a document released by The Intercept, detailing the schedule of a recent "CEO Summit" of 28 IQT portfolio companies concluded in February. From the itinerary, the standout companies provided "unique tools to mine data from platforms such as Twitter."

PATHAR

PATHAR has a product called "Dunami" that monitors social media sites for "networks of association, centers of influence and potential signs of radicalization." These social media sites include, but are not limited to, Facebook, Twitter, and Instagram.

TransVoyant

TransVoyant offers procedures that analyze multiple data points to determine potential "decision-makers" who could organize "gang incidents" and situations threatening to the press. The tech company recently worked with the U.S. military to utilize satellite, radar, and drone surveillance data.

Databricks

Ex. 9-1

Databricks' "Spark" can sort through big chunks of data rapidly, which the International Business Machine (IBM) has labeled as "the most significant open source project of the next decade." The tech company utilizes the cloud to host "big data analytics and processing platforms."

Dataminr

Dataminr has automated learning machines that mark trends in streams from Twitter by cross-referencing data gathered from other unusual clusters. These processes "directly license" Twitter data streams, for clients such as police departments, to "visualize" any sign of purported tendencies.

Geofeedia

Geofeedia employs geotagging technology to monitor real-time movements, such as Greenpeace mobilizations, student protests, minimum wage rallies and other political activities. The data is utilized by corporations, including McDonald's and the Mall of America, and law enforcement agencies in Detroit, Oakland, and Chicago, among other police departments.

A Violation of Privacy Rights?

Senior staff attorney from the American Civil Liberties Union, Lee Rowland, believes such surveillance tactics employed by the CIA and other government bodies, along with private sectors, may infringe upon the public's rights due to unwarranted suspicion.

"The courts have rightly recognized that when millions of bits of data are aggregated into a dossier about your behavior, that is no longer properly public and violates privacy rights," said Rowland.

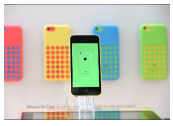
"When you have private companies deciding which algorithms get you a so-called threat score, or make you a person of interest, there's obviously room for targeting people based on viewpoints or even unlawfully targeting people based on race or religion," Rowland explained.

Photo: Ludovic Bertron | Flickr

TAG CIA , surveillance , Social Media , Twitter , Instagram

RELATED ARTICLES

Racial Bias Still Plagues Chicago Police: Task Force Report



FBI Reportedly Hired Professional Hackers To Crack San Bernardino iPhone

FBI Director Covers His Laptop's Webcam With Tape: Why? Should You Do It?

CIA Says No More Waterboarding, Not Even With Orders From US President

WikiLeaks Publishes CIA Director John Brennan's Hacked Emails, Including Private Information Of Family And Associates

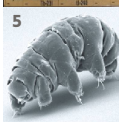
MOST POPULAR

EARTH/ENVIRONMENT
Mysterious Shift In Earth's Field Prompts Scientists T Magnetic Model That Gui

ANCIENT
Artificial Intelligence Ider Ancestor Species That Wa Hybrid Of Neanderthals A

ANCIENT
Scientists Say Pair Of Anc Skeletons Found In South From Same Species

FEATURE | SCIENCE
World's Oldest Periodic T Dating Back To 1885 Foun Room Of British Universit



ANIMALS
Bodies Of Tardigrades, Cr Found In Antarctica's Lak

Viral 10-Year Challenge Sparks Wave Of C Posts On Social Media

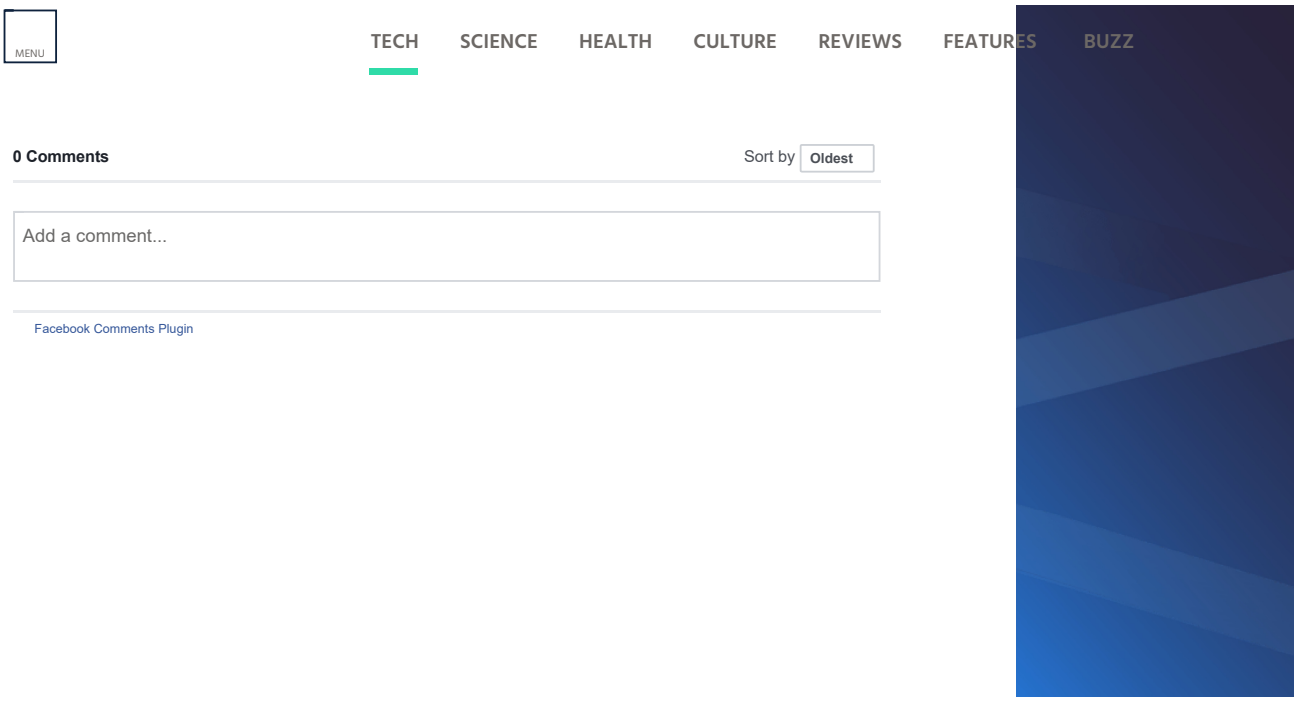
Scientists Say Pair Of Ancient Hominin Sk In South Africa Are From Same Species

Turns Out The iPhone X Can Fit Into The i Battery Case Just Fine

Harvard Professor Avi Loeb Justifies Why Object 'Oumuamua Is An Alien Probe

Artificial Intelligence Identifies Human Ar That Was Likely A Hybrid Of Neanderthal Denisovans

Ex. 9-2



Ex. 9-3

EXHIBIT 10

Raimond Ranne, DBA, MPA • 3rd

Law Enforcement Professional, Intel Analyst, Homeland Security Professional, Educator and Manager

Palatine Police Department • Argosy University Chicago

Greater Chicago Area • 500+

Send InMail

A highly regarded, decorated, dedicated, and knowledgeable Law Enforcement professional assigned as an intelligence analyst with extensive experience in vulnerability/threat assessments, investigations, open source analysis, emergency preparedness including numerous certifications and hands-on experience safeguarding the public, corporations, and country utilizing technological platforms such as Lexisnexis, Tweetdeck, Pathar/Dunami, Vigilant/LEARN, CANVAS, Facial Recognition, Accurint, Genetec and others. Seeking new opportunities in Emergency Management/Consulting/Training.

Security & Threat Assessments, Investigations, Risk Mitigation, Strategic & Tactical Plans, Emergency Preparedness & Response, Homeland Security, Corporate Investigations, Program Development, Presentations & Public Speaking, Team & Consensus Building, Training & Development, Curriculum Development, Physical & Digital Security

See less

Raimond's Activity

Great event hosted by the Dallas Cowboys and #ASIS17...
Raimond liked

Like & Comment if you Agree #LouisSpagnuolo #Influencer #CEO
Raimond liked

Aviation Benefits 2017 - Industry High Level Group Report
Raimond liked

Attending the Rosecrance Florian Symposium. Focused on wellness and
Raimond liked

Chicago Meigs Field, once upon a time ...
Raimond liked

PR Police
Raimond liked

See all activity

Experience

Police Assistant
Palatine Police Department
May 2017 – Present • 5 mos
Palatine, Illinois

Analyst/Police Officer
City of Chicago
Nov 1991 – May 2017 • 25 yrs 7 mos

Contact and Personal Info

Raimond's Profile

Show more

People Also Viewed

Bruce M. Rottner • 3rd
Experienced Police Executive

Lt. Ozzie Valdez • 3rd
Homicide Lieutenant / Chicago P
Department, Advanced Specialist
The Behavioral Analysis of Force
Encounters

David DiSanti • 3rd
Patrolman at Chicago Police Department

Berscott Ruiz • 3rd
Police Officer

Mic Fallon • 3rd
CRIMINAL AND CIVIL INVESTIGATO

Dave Dunham • 3rd
Chief Marketing Officer at Chicag
Patrolmen's

Phil Kwasinski • 3rd
Captain Chicago Police Departme

Hector Rodriguez • 3rd
Chief - Real Estate Investigations,
Illinois Department of Financial &
Professional Regulation

Jennifer Rottner • 3rd
Director of Communications at Ci
Chicago Department of Family an
Support Services

Martin Bappert • 3rd
Handyman/Carpenter

Learn the skills Raimond has

Managing Customer Expectations for Frontline Employees
Viewers: 14,609

Messaging

Train, motivate, and certify corporate and community volunteers to become Community Emergency Response Team (CERT) members. Serve as active Certified Department of Homeland Security (DHS) Safety Officer, and member of City of Chicago Incident Management Team (IMT), Intelligence analyst (CPIC).

Creates centers of excellence in safety and security, spearheading sophisticated assessments and strategies.
Protects interests and assets, identifying and developing robust controls for threats, risks, and vulnerabilities.
Amplifies knowledge and awareness, designing and effectively communicating value of programs and initiatives.
Galvanizes people on all levels on common missions and goals, conducting clear and engaging presentations.
Builds, develops, and mobilizes high-performance teams, serving as educator, trainer, and leader by example.

Analyst
City of Chicago
Nov 1991 – May 2017 • 25 yrs 7 mos

Currently assigned as an Open Source/Intelligence Analyst, Operations Command (CPIC). Develop/conduct safety seminars and presentations for internal and external audiences on all levels. Provide a full range of security, risk, threat, and vulnerability assessments, mitigation planning/execution, emergency management, and disaster response for corporations, businesses, and civic organizations, as well as the public.
KEY CONTRIBUTIONS:
• Train, motivate, and certify corporate and community volunteers to become Community Emergency Response Team (CERT) members.
• Served as a Department of Homeland Security (DHS) Safety Officer, and as a member of the City of Chicago Incident Management Team (IMT).

Training and Certifications obtained:

NIMS, ICS Level 100,200,300,400,700,800 All Hazards Certification.
FEMA Emergency Management Institute Training, Emmitsburg, Maryland.
FEMA Professional Development Series Certification
FEMA IS130 Exercise Evaluation and Improvement Planning Certification
Certified Department of Homeland Security Safety Officer, Incident Commander training.
IRTB (Incident Response to Terrorist Bombing) Instructor.
C.E.R.T. (Community Emergency Response Team) Instructor.
IPMBA (International Mountain Bike Association) Instructor and past Board member.
Department of Homeland Security Weapons of Mass Destruction: Radiological/Nuclear Awareness Instructor
FBI Facial Recognition Training.
NHTSA (National Highway Transportation Safety Administration) Instructor.
CIKR Critical Infrastructure and Key Resources Training.
U.S. Department of Homeland Security/Louisiana State University-Terrorist Deterrence Training
U.S. Department of Energy/University of Nevada Las Vegas Radiological/Nuclear Awareness Training
Department of Homeland Security/New Mexico Tech Initial Law Enforcement Response to Suicide Bombing Attacks (ILERSBA) Training
Department of Justice Terrorism Investigations and Intelligence.
Psychology of Terrorism and Terrorism Victims Training.

Adjunct Professor
Argosy University
May 2010 – 2016 • 6 yrs
Chicago

Adjunct Professor:
Undergraduate Criminal Justice- (Emergency Management, Homeland Security, Criminal Justice Research)

Undergraduate Business Administration- (Marketing, Human Resources)

Graduate Business Administration- (Project Management, Communication Strategies for Managers, Leadership in Public and Non-Profit Organizations)

Adjunct Professor
DeVry University
2010 – 2011 • 1 yr

Adjunct Professor in the College of Business

See more positions

Education

Argosy University Chicago
Doctor of Business Administration, International Business/Emergency Management

Dissertation: Private Sector Emergency Disaster Response: An Examination of Adopting CERT Into Emergency Response Planning

Calumet College of Saint Joseph
M.S., Public Safety Administration

B.S. Law Enforcement Management

Calumet College of Saint Joseph
Bachelor of Science (B.S.) Law Enforcement Administration

Volunteer Experience

Board Member
International Police Mountain Bike Association
1996 – 2000 • 4 yrs
Education

Board Member, Served as Industry Liasion

Basketball Coach
Oriole Park Elementary School
Children

Little League Baseball Coach
Oriole Park Baseball Association
Children

Featured Skills & Endorsements

Homeland Security · 66

Endorsed by **Thomas Tilton and 8 others who are highly skilled at this**

Endorsed by **2 of Raimond's colleagues at City of Chicago**

Emergency Mana... · 62

Endorsed by **Rick Hoyer, Ph.D., Psy.D., Ed.D. and 6 others who are highly skilled at this**

Endorsed by **5 of Raimond's colleagues at City of Chicago**

Criminal Justice · 37

Endorsed by **Peter J. Piazza and 6 others who are highly skilled at this**

Endorsed by **2 of Raimond's colleagues at City of Chicago**

View 47 more

Messaging

Messaging

EXHIBIT 11

Geofeedia cuts half of staff after losing access to Twitter, Facebook

Twitter has cut off Geofeedia's access to its data after a report found that law enforcement has been using Geofeedia to monitor activists and protesters.

By **Amina Elahi**
Blue Sky Innovation

NOVEMBER 21, 2016, 5:16 PM

Chicago-based Geofeedia, a CIA-backed social-media monitoring platform that drew fire for enabling law enforcement surveillance, has let go 31 of its approximately 60 employees, a spokesman said Tuesday.

In mid-October, Twitter followed Facebook and Instagram in cutting Geofeedia off from its valuable data stream, after an American Civil Liberties Union report said police had used the platform to track protests and other large gatherings. The Chicago Police Department and others have used the company's tools.

Ex. 11-1

Geofeedia cut the jobs, mostly in sales in the Chicago office, in the third week of October, the spokesman said. It has offices in Chicago, Indianapolis and Naples, Fla. The cuts were first reported by Crain's Chicago Business.

An emailed statement attributed to CEO Phil Harris said Geofeedia wasn't "created to impact civil liberties," but in the wake of the public debate over their product, they're changing the company's direction.

"Following these suspensions, we have decided to scale back our business and focus on a variety of innovations that will allow us to serve our customers and continue our rapid growth trajectory as a leading real-time analytics and alerting platform," the statement said.

Harris said Geofeedia's software has been "impactful" for schools, sports leagues, customer service, marketing and event planning, per the statement. He also referred to the company's $17 million funding round in February — which brought its total funding to nearly $24 million — and "strong sales and growth" as strengthening the company.

"Our strong financial position has allowed us to carefully consider the appropriate areas of focus for our technology going forward," Harris wrote in the statement.

Geofeedia would not say if it lost clients following the ACLU report, and declined to specify what areas it will focus on moving forward.

aelahi@tribpub.com
Twitter @aminamania

This 'attr(data-c-typename)' is related to: Job Layoffs, Unemployment and Layoffs

EXHIBIT 12

Rahm Emanuel
Mayor

Department of Police · City of Chicago
3510 S. Michigan Avenue · Chicago, Illinois 60653

Eddie T. Johnson
Superintendent of Police

November 18, 2016

Rachel Murphy
ACLU
Response Via Email: rmurphy@aclu-il.org

Re: NOTICE OF RESPONSE TO FOIA REQUEST
REQUEST DATE: October 19, 2016
FOIA FILE NO.: P053313

Dear Ms. Murphy,

The Chicago Police Department (CPD) is in receipt of your Freedom of Information Act ("FOIA") request. CPD contacted you on October 31, 2016, where you agreed to extend CPD's time to respond until November 18, 2016. Please note that this response was submitted within the extended deadline of November 18, 2016. In your request, you state the following:

We write to seek information about the Chicago Police Department's records[1] regarding software designed to access information from social media services[2], as defined herein

> *"1. All records referencing grant applications, budget requests, loans, donations or other funding for software designed to access information from social media services. 2. All records referencing meeting agendas or minutes, public notice, analyses, communications between law enforcement and elected leaders, or other public process related to the acquisition of software designed to access information from social media services. 3. All records referencing the purchase of, acquisition of, installation of, subscription to, payment for, or agreements for software designed to access information from social media services. 4. All records referencing product features or the functioning of software designed to access information from social media services. 5. All records referencing correspondence with any company or company representative regarding software designed to access*

[1] Throughout this request the term "records" includes but is not limited to any paper or electronic information, reports, evaluation, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas, meeting minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, or other similar materials.

[2] Throughout this request, the term "software designed to access information from social media services" includes but is not limited to software that enables the monitoring, searching, collection, or analysis of user-generated content located on social media services. Examples of such social medial services include but are not limited to Facebook, Instagram, Twitter, Google Plus, Pinterest, Yik Yak, Reddit, SnapChat, and MySpace. "Software designed to access information from social medial services" does not include a mobile application or website operated by a social media service.

information from social media services. 6. All records referencing policies governing access, use, or training related to software designed to access information from social media services. 7. All records referencing the sharing with entities outside of your department of information collected through the use of software designed to access information from social media services. 8. All records referencing social media profiles or content accessed, viewed, or retained through the use of software designed to access information from social media services. 9. All records referencing the locations or geographic areas viewed, searched, or monitored through the use of software designed to access information from social media services."

With regard to your request as a whole, processing such a request would be unduly burdensome as written. FOIA provides in 5 ILCS 140/3(g) that requests for all records falling within a category shall be complied with unless compliance with the request would be unduly burdensome for the complying body and there is no way to narrow the request and the burden on the public body outweighs the public interest in the information. Given its breadth and ambiguity, thousands of pages of responsive documentation could potentially fall with the scope of this request and its attendant definitions. Identifying, locating, and compiling all such tangentially related material would easily take CPD many weeks to complete. Assuming, *arguendo*, this incredible task could be completed, all responsive documentation would need to be reviewed for information that is exempt under FOIA and other relevant state and federal statutes. Based on past requests, it would be reasonable to expect a trained FOIA officer to take at least one minute to review one page of responsive documents. Reviewing all responsive documents in the aggregate would consequently require well in excess of 50 hours to complete such a demanding task. The short response time allowed by FOIA makes the task of identifying, collecting, and reviewing potentially responsive records in a timely manner unduly burdensome upon CPD. As a result, CPD has determined that compliance with your request in the aggregate is unduly burdensome and that CPD's burden to process your request outweighs the public's interest.

Nevertheless, CPD has taken measures to reasonably comply with such a broad request. In order to determine whether your request could be complied with, this matter was directed to several different entities within the Department. In response to items 1 and 3, regarding your request for information pertaining to grants and purchase orders for software designed to access information from social media services, the CPD Finance Division was able to produce the relevant contracts and purchase orders. Finance has indicated that current contracts are available from the City of Chicago Procurement Services Department website. Under FOIA, a "public body is not required to copy a public record that is published on the public body's website," so long as the requestor is directed to that website. 5 ILCS 140/8.5. This informational database can be accessed and searched at:

https://www.cityofchicago.org/city/en/depts/dps/provdrs/contract/svcs/awarded_contracts.html

In response to item 2, regarding your request for records of meeting agendas or minutes, public notice, analyses, and communications between law enforcement and elected leaders pertaining to social media tracking software has also been reviewed by the CPD Crime Prevention and Information Center (CPIC). CPIC has indicated that CPD does not conduct such meetings or communications, and thus retains no responsive records pertaining to this portion of your request. Please note that FOIA requires public bodies to provide *existing* public records. *See* 5 ILCS 140/3(a) ("Each public body shall make available to any person for inspection or copying all public records, except as otherwise provided in Sections 7 and 8.5 of this Act."). FOIA does not require public bodies to create records, or compile information for the purpose of creating a record.

In response to items 4, 6 and 7 of your request, regarding records referencing product features and function of social media tracking software, records referencing policies governing access or training related to such software, and records referencing the sharing of information collected through the use of such software, CPIC has provided its software user guide, social media directives and privacy policies. These documents can also be accessed from the Department's Directives System:

http://directives.chicagopolice.org/directives/

Regarding items 8 and 9 of your request, CPIC has also reviewed your request for records referencing social media profiles or content accessed by the aforementioned software, as well as your request for records referencing the locations or geographic areas viewed, searched or monitored through the use of such software. In response to these requests, CPIC has provided the Open Source receipts for its searches of social media, as well as the maps of areas that were searched through social media tracking software. Please bear in mind that it is CPIC's practice to maintain Open Source receipts for thirty days; as such, you are being provided with the 30 days of records preceding November 2, 2016, the date your request was processed. Concerning the maps of search areas: the aforementioned software creates no permanent record of these graphics. For demonstrative purposes, CPIC has created a screen-shot of such maps that were generated over the course of November 10, 2016. At this time, the aforementioned documents from Finance and CPIC are being provided to you. Certain information has been redacted from these documents pursuant to the Act; these redactions are explained as follows.

Home addresses and signatures were redacted pursuant to section 7(1)(b) which exempts from disclosure, "[p]rivate information, unless disclosure is required by another provision of this Act, a State or federal law or a court order." 5 ILCS 140/7(1)(b). "Private information" is defined in section 2(c-5) as "unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person." 5 ILCS 140/2(c-5). Therefore, employee numbers and signatures were properly redacted section 7(1)(b).

Dates of birth as well as names and images of individuals who incidentally appear in reports have been redacted pursuant to Section 7(1)(c) of FOIA. 5 ILCS 140/7(1)(c) exempts from disclosure, "[p]ersonal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information." Individuals who incidentally appear in the reports have a strong interest in keeping their identity private and therefore their names were properly redacted pursuant to Section 7(1)(c) of FOIA. Moreover, dates of birth are highly personal and were also properly redacted pursuant to Section 7(1)(c) of FOIA 5 ILCS 140/70(1)(c).

Names, addresses and other information that could be used to identify witnesses is exempt pursuant to Section 7(1)(d)(iv) which exempts law enforcement records where release would "unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies." 5 ILCS 140/7(1)(d)(iv).

Names of social media tracking software were redacted pursuant to Section 7(1)(d)(v) which exempts records that would, "[d]isclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request." 5 ILCS 140/7(1)(d)(v). In order to meet this standard, the claimant must demonstrate that the investigative technique is not generally used and known, and that such disclosure would lead to demonstrable harm to the public body. The first element of this standard is easily met, as CPIC utilizes software programs that, unlike Geofeedia, are not generally used and known to the public. Meeting the second element can also be met, as past disclosures of social media tracking software have led to lasting damage to the Department. In the wake of news that CPD utilizes Geofeedia to track open source social media accounts, numerous users of social media sites took action to restrict public access to their accounts. Once this mass "lock-out" occurred, Geofeedia lost its utility as a specialized

investigative technique, preventing CPIC from carrying out its duties regarding crime prevention strategy. Given that these social media monitoring tools have great worth in identifying shooting victims and perpetrators, it would be incredibly damaging to the Department's police powers if these tools were publicly identified. As such, these names must be withheld pursuant to 7(1)(d)(v).

Moreover, 5 ILCS 140/7(1)(g) exempts from disclosure, "[t]rade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested." Given the current business climate, the production of materials that mention the name of the business in this instance would destroy the company's business. These materials reveal non-public details about the company's product pricing and services. If disclosed, that pricing information would permit competitors to undercut our offerings, or could generate controversies amount the Company's clients. Either possibility would dissuade a company form contracting with CPD going forward, resulting in both harm to the company and the Department's investigating efforts. The materials further disclose non-public commercial and financial information where disclosure would likely allow competitors to reverse engineer the company's services.

To the extent you seek email correspondence, your request requires further information. Parameters that would assist CPD in conducting an email search include: (1) the name or e-mail address of the account you wish searched; (2) key words you wish to search for; (3) the e-mail address of each individual's mailbox, if you seek e-mail correspondence to and from two individuals; and (4) the timeframe to be searched. Here, you indicate that you would like emails related to social media tracking software. In order to determine whether such a search could be conducted, your request was forwarded to the CPD Bureau of Support Services: Information Services Division. Information Services has indicated that an email search of the CPD email system would require identification of the individuals whose email accounts are to be searched, the full timeframe you would like to have searched, and any key terms that are to be searched. At this point, none of these variables are specified in this request. It should be emphasized that the Act neither requires nor allows CPD to speculate as to the details of any request; this information can only be provided by the petitioner.

Pursuant to section 3(g) of FOIA, we would like to extend to you an opportunity to modify your request to make it more manageable. Unless and until a new FOIA request is submitted that specifies what records you are seeking, CPD will be unable to process your petition. CPD encourages you to review your request to ascertain the details of your query. Once this is determined, a new FOIA request can be submitted to CPD, specifying the records you would like CPD to provide. If we do not receive your narrowed request within seven calendar days of the date of this letter, your request in the aggregate will be denied.

In the event that responsive information has been exempted by CPD, such decisions may be reviewed by the Public Access Counselor (PAC) at the Office of the Illinois Attorney General, 500 S. 2nd Street, Springfield, Illinois 62706, (877) 299-3642. You also have the right to seek judicial review of your denial by filing a lawsuit in the Circuit Court of Cook County. Any and all appeals to the Circuit Court of Cook County must be filed within two years of the alleged violation.

If you require additional assistance, feel free to contact this office.

Sincerely,

Dane J. Rohrer
Freedom of Information Officer

City of Chicago Department of Police
Office of Legal Affairs-FOIA Unit
3510 South Michigan, Fourth Floor
Chicago, Illinois 60653
(312) 745-5308
foia@chicagopolice.org

EXHIBIT 13

STATE OF ILLINOIS
93rd GENERAL ASSEMBLY
HOUSE OF REPRESENTATIVES
TRANSCRIPTION DEBATE

69th Legislative Day 5/31/2003

Speaker Madigan: "The House shall come to order. The Members shall be in their chairs. We ask you to turn off your cell phones, your computers, your pagers. We ask the guests in the gallery to rise and join us for the invocation. We shall be led in prayer today by Lee Crawford, the Assistant Pastor of the Victory Temple Church in Springfield."

Pastor Crawford: "Let us pray. Most gracious and sovereign King, we so humbly come before You giving You praise for all things. For Your word says that we are to bless the Lord at all times and that Your praises should and will continually to be in our mouths. Father, we praise You with the confidence that all things work together for the good of them who love God and are called according to Your purpose. Father, we realize that some things we cannot control, but we also realize that You, O Lord, are in control of all things. So, we place our trust and our confidence in You. This we ask in Your Son's name. Amen."

Speaker Madigan: "We shall be led in the Pledge of Allegiance by Representative Ken Dunkin."

Dunkin - et al: "I pledge allegiance to the Flag of the United States of America and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all."

Speaker Madigan: "Roll Call for Attendance. Representative Currie."

Currie: "Thank you, Speaker. I have no excused absences to report today."

Speaker Madigan: "Mr. Bost."

'no'. The voting is open. Have all voted who wish? Have all voted who wish? Have all voted who wish? Mr. Parke. Mr. Acevedo. Mr. Clerk, take the record. On this question, there are 115 voting 'yes', 0 voting 'no', 0 voting 'present'. And the House does concur in Senate Amendments #4 to House Bill 294. And having reached the required Majority, is hereby declared passed. On page 22 of the Calendar, on the Order of Concurrences, there's House Bill 954. The Gentleman from Will, Mr. Meyer, on a Concurrence Motion. Mr. Meyer."

Meyer: "Thank you, Mr. Speaker, Ladies and Gentlemen of the House. House Bill 954 is identical… First, I move to concur in Senate Amendment 1 to House Bill 954. It is identical to House Bill 305 which passed out of the House unanimously. It went to the Senate. They did nothing with it there except they amended it on to House Bill 954 as opposed to passing it as House Bill 305. It was drafted by the Attorney General's Office and represents two years of negotiations with the Illinois Press Association, the Peoples Energy, Illinois Municipal League, the DuPage Mayors and Managers Conference, City of Chicago and Illinois Power. It's also supported by EMA and it amends the Open Meetings Act and FOIA to allow public bodies to hold closed meetings when considering homeland security issues, exempts documents prepared for emergency and security procedures from being disclosed from homeland security where that would be compromised. Again, it's

passed out of here unanimously and passed in the Senate the same way in this form. I'd appreciate an 'aye' vote."

Speaker Novak: "Is there any discussion? The Gentleman now moves that the House concur in Senate Amendments #1 to House Bill 954. All those in favor vote 'aye'; all those opposed vote 'no'. The voting is open. Have all voted who wish? Have all voted who wish? Have all voted who wish? Mr. Clerk, take the record. On this question, there are 115 voting 'yes', 0 voting 'no', 0 voting 'present'. And the House does concur in Senate Amendment #1 to House Bill 954. And having reached the required Majority, is hereby declared passed. On page 20 of the Calendar is House Bill 318 on a Motion to Nonconcur. Representative Yarbrough. Thank you."

Yarbrough: "That's a nonconcurrence?"

Speaker Novak: "Yes, this is a Motion to Nonconcur, Representative."

Yarbrough: "Okay, thank you. Thank you, Mr. Speaker. I'd like to nonconcur with the Amendment, the Senate Amendment #1."

Speaker Novak: "The Lady moves to nonconcur in Senate Amendments #1. Is there any discussion? Seeing none, the question is, 'Shall the House nonconcur in Senate Amendments #1 to House Bill 318?' All those in favor say 'aye'; all those opposed say 'no'. The 'ayes' have it. And the House nonconcurs in Senate Amendments #1 to House Bill 318. On page 22 of the Calendar, on the Order of Concurrences, there is House Bill 983. The Gentleman from Cook, Mr. Lang on the Concurrence Motion."

EXHIBIT 14

AN ACT in relation to freedom of information.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 5. The Open Meetings Act is amended by changing Section 2 as follows:

(5 ILCS 120/2) (from Ch. 102, par. 42)

Sec. 2. Open meetings.

(a) Openness required. All meetings of public bodies shall be open to the public unless excepted in subsection (c) and closed in accordance with Section 2a.

(b) Construction of exceptions. The exceptions contained in subsection (c) are in derogation of the requirement that public bodies meet in the open, and therefore, the exceptions are to be strictly construed, extending only to subjects clearly within their scope. The exceptions authorize but do not require the holding of a closed meeting to discuss a subject included within an enumerated exception.

(c) Exceptions. A public body may hold closed meetings to consider the following subjects:

(1) The appointment, employment, compensation, discipline, performance, or dismissal of specific employees of the public body, including hearing testimony on a complaint lodged against an employee to determine its validity.

(2) Collective negotiating matters between the public body and its employees or their representatives, or deliberations concerning salary schedules for one or more classes of employees.

(3) The selection of a person to fill a public office, as defined in this Act, including a vacancy in a

public office, when the public body is given power to appoint under law or ordinance, or the discipline, performance or removal of the occupant of a public office, when the public body is given power to remove the occupant under law or ordinance.

(4) Evidence or testimony presented in open hearing, or in closed hearing where specifically authorized by law, to a quasi-adjudicative body, as defined in this Act, provided that the body prepares and makes available for public inspection a written decision setting forth its determinative reasoning.

(5) The purchase or lease of real property for the use of the public body, including meetings held for the purpose of discussing whether a particular parcel should be acquired.

(6) The setting of a price for sale or lease of property owned by the public body.

(7) The sale or purchase of securities, investments, or investment contracts.

(8) Security procedures and the use of personnel and equipment to respond to an actual, a threatened, or a reasonably potential danger to the safety of employees, students, staff<u>, the public,</u> or public property.

(9) Student disciplinary cases.

(10) The placement of individual students in special education programs and other matters relating to individual students.

(11) Litigation, when an action against, affecting or on behalf of the particular public body has been filed and is pending before a court or administrative tribunal, or when the public body finds that an action is probable or imminent, in which case the basis for the finding shall be recorded and entered into the minutes of the closed meeting.

(12) The establishment of reserves or settlement of claims as provided in the Local Governmental and Governmental Employees Tort Immunity Act, if otherwise the disposition of a claim or potential claim might be prejudiced, or the review or discussion of claims, loss or risk management information, records, data, advice or communications from or with respect to any insurer of the public body or any intergovernmental risk management association or self insurance pool of which the public body is a member.

(13) Conciliation of complaints of discrimination in the sale or rental of housing, when closed meetings are authorized by the law or ordinance prescribing fair housing practices and creating a commission or administrative agency for their enforcement.

(14) Informant sources, the hiring or assignment of undercover personnel or equipment, or ongoing, prior or future criminal investigations, when discussed by a public body with criminal investigatory responsibilities.

(15) Professional ethics or performance when considered by an advisory body appointed to advise a licensing or regulatory agency on matters germane to the advisory body's field of competence.

(16) Self evaluation, practices and procedures or professional ethics, when meeting with a representative of a statewide association of which the public body is a member.

(17) The recruitment, credentialing, discipline or formal peer review of physicians or other health care professionals for a hospital, or other institution providing medical care, that is operated by the public body.

(18) Deliberations for decisions of the Prisoner Review Board.

(19) Review or discussion of applications received under the Experimental Organ Transplantation Procedures Act.

(20) The classification and discussion of matters classified as confidential or continued confidential by the State Employees Suggestion Award Board.

(21) Discussion of minutes of meetings lawfully closed under this Act, whether for purposes of approval by the body of the minutes or semi-annual review of the minutes as mandated by Section 2.06.

(22) Deliberations for decisions of the State Emergency Medical Services Disciplinary Review Board.

(23) The operation by a municipality of a municipal utility or the operation of a municipal power agency or municipal natural gas agency when the discussion involves (i) contracts relating to the purchase, sale, or delivery of electricity or natural gas or (ii) the results or conclusions of load forecast studies.

(d) Definitions. For purposes of this Section:

"Employee" means a person employed by a public body whose relationship with the public body constitutes an employer-employee relationship under the usual common law rules, and who is not an independent contractor.

"Public office" means a position created by or under the Constitution or laws of this State, the occupant of which is charged with the exercise of some portion of the sovereign power of this State. The term "public office" shall include members of the public body, but it shall not include organizational positions filled by members thereof, whether established by law or by a public body itself, that exist to assist the body in the conduct of its business.

"Quasi-adjudicative body" means an administrative body charged by law or ordinance with the responsibility to conduct hearings, receive evidence or testimony and make

determinations based thereon, but does not include local electoral boards when such bodies are considering petition challenges.

(e) Final action. No final action may be taken at a closed meeting. Final action shall be preceded by a public recital of the nature of the matter being considered and other information that will inform the public of the business being conducted.

(Source: P.A. 90-144, eff. 7-23-97; 91-730, eff. 1-1-01.)

Section 10. The Freedom of Information Act is amended by changing Section 7 as follows:

(5 ILCS 140/7) (from Ch. 116, par. 207)

Sec. 7. Exemptions.

(1) The following shall be exempt from inspection and copying:

(a) Information specifically prohibited from disclosure by federal or State law or rules and regulations adopted under federal or State law.

(b) Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy. Information exempted under this subsection (b) shall include but is not limited to:

(i) files and personal information maintained with respect to clients, patients, residents, students or other individuals receiving social, medical, educational, vocational, financial, supervisory or custodial care or services directly

or indirectly from federal agencies or public bodies;

(ii) personnel files and personal information maintained with respect to employees, appointees or elected officials of any public body or applicants for those positions;

(iii) files and personal information maintained with respect to any applicant, registrant or licensee by any public body cooperating with or engaged in professional or occupational registration, licensure or discipline;

(iv) information required of any taxpayer in connection with the assessment or collection of any tax unless disclosure is otherwise required by State statute; and

(v) information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agencies; provided, however, that identification of witnesses to traffic accidents, traffic accident reports, and rescue reports may be provided by agencies of local government, except in a case for which a criminal investigation is ongoing, without constituting a clearly unwarranted per se invasion of personal privacy under this subsection.

(c) Records compiled by any public body for administrative enforcement proceedings and any law enforcement or correctional agency for law enforcement purposes or for internal matters of a public body, but only to the extent that disclosure would:

(i) interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional

agency;

(ii) interfere with pending administrative enforcement proceedings conducted by any public body;

(iii) deprive a person of a fair trial or an impartial hearing;

(iv) unavoidably disclose the identity of a confidential source or confidential information furnished only by the confidential source;

(v) disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents of correctional agencies related to detection, observation or investigation of incidents of crime or misconduct;

(vi) constitute an invasion of personal privacy under subsection (b) of this Section;

(vii) endanger the life or physical safety of law enforcement personnel or any other person; or

(viii) obstruct an ongoing criminal investigation.

(d) Criminal history record information maintained by State or local criminal justice agencies, except the following which shall be open for public inspection and copying:

(i) chronologically maintained arrest information, such as traditional arrest logs or blotters;

(ii) the name of a person in the custody of a law enforcement agency and the charges for which that person is being held;

(iii) court records that are public;

(iv) records that are otherwise available under State or local law; or

(v) records in which the requesting party is the individual identified, except as provided under part (vii) of paragraph (c) of subsection (1) of this Section.

"Criminal history record information" means data identifiable to an individual and consisting of descriptions or notations of arrests, detentions, indictments, informations, pre-trial proceedings, trials, or other formal events in the criminal justice system or descriptions or notations of criminal charges (including criminal violations of local municipal ordinances) and the nature of any disposition arising therefrom, including sentencing, court or correctional supervision, rehabilitation and release. The term does not apply to statistical records and reports in which individuals are not identified and from which their identities are not ascertainable, or to information that is for criminal investigative or intelligence purposes.

(e) Records that relate to or affect the security of correctional institutions and detention facilities.

(f) Preliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body. The exemption provided in this paragraph (f) extends to all those records of officers and agencies of the General Assembly that pertain to the preparation of legislative documents.

(g) Trade secrets and commercial or financial information obtained from a person or business where the trade secrets or information are proprietary, privileged or confidential, or where disclosure of the trade secrets or information may cause competitive harm, including all

information determined to be confidential under Section 4002 of the Technology Advancement and Development Act. Nothing contained in this paragraph (g) shall be construed to prevent a person or business from consenting to disclosure.

(h) Proposals and bids for any contract, grant, or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person proposing to enter into a contractor agreement with the body, until an award or final selection is made. Information prepared by or for the body in preparation of a bid solicitation shall be exempt until an award or final selection is made.

(i) Valuable formulae, computer geographic systems, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss.

(j) Test questions, scoring keys and other examination data used to administer an academic examination or determined the qualifications of an applicant for a license or employment.

(k) Architects' plans, ~~and~~ engineers' technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for projects constructed or developed with public funds, but only to the extent that disclosure would compromise security.

(l) Library circulation and order records identifying library users with specific materials.

(m) Minutes of meetings of public bodies closed to the public as provided in the Open Meetings Act until the public body makes the minutes available to the public under Section 2.06 of the Open Meetings Act.

(n) Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies.

(o) Information received by a primary or secondary school, college or university under its procedures for the evaluation of faculty members by their academic peers.

(p) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(q) Documents or materials relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.

(r) Drafts, notes, recommendations and memoranda pertaining to the financing and marketing transactions of the public body. The records of ownership, registration, transfer, and exchange of municipal debt obligations, and of persons to whom payment with respect to these obligations is made.

(s) The records, documents and information relating

to real estate purchase negotiations until those negotiations have been completed or otherwise terminated. With regard to a parcel involved in a pending or actually and reasonably contemplated eminent domain proceeding under Article VII of the Code of Civil Procedure, records, documents and information relating to that parcel shall be exempt except as may be allowed under discovery rules adopted by the Illinois Supreme Court. The records, documents and information relating to a real estate sale shall be exempt until a sale is consummated.

(t) Any and all proprietary information and records related to the operation of an intergovernmental risk management association or self-insurance pool or jointly self-administered health and accident cooperative or pool.

(u) Information concerning a university's adjudication of student or employee grievance or disciplinary cases, to the extent that disclosure would reveal the identity of the student or employee and information concerning any public body's adjudication of student or employee grievances or disciplinary cases, except for the final outcome of the cases.

(v) Course materials or research materials used by faculty members.

(w) Information related solely to the internal personnel rules and practices of a public body.

(x) Information contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of a public body responsible for the regulation or supervision of financial institutions or insurance companies, unless disclosure is otherwise required by State law.

(y) Information the disclosure of which is restricted under Section 5-108 of the Public Utilities

Act.

(z) Manuals or instruction to staff that relate to establishment or collection of liability for any State tax or that relate to investigations by a public body to determine violation of any criminal law.

(aa) Applications, related documents, and medical records received by the Experimental Organ Transplantation Procedures Board and any and all documents or other records prepared by the Experimental Organ Transplantation Procedures Board or its staff relating to applications it has received.

(bb) Insurance or self insurance (including any intergovernmental risk management association or self insurance pool) claims, loss or risk management information, records, data, advice or communications.

(cc) Information and records held by the Department of Public Health and its authorized representatives relating to known or suspected cases of sexually transmissible disease or any information the disclosure of which is restricted under the Illinois Sexually Transmissible Disease Control Act.

(dd) Information the disclosure of which is exempted under Section 30 of the Radon Industry Licensing Act.

(ee) Firm performance evaluations under Section 55 of the Architectural, Engineering, and Land Surveying Qualifications Based Selection Act.

(ff) Security portions of system safety program plans, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority under Section 2.11 of the Regional Transportation Authority Act or the St. Clair County Transit District under the Bi-State Transit Safety Act.

(gg) Information the disclosure of which is restricted and exempted under Section 50 of the Illinois Prepaid Tuition Act.

(hh) Information the disclosure of which is exempted under Section 80 of the State Gift Ban Act.

(ii) Beginning July 1, 1999, information that would disclose or might lead to the disclosure of secret or confidential information, codes, algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.

(jj) Information contained in a local emergency energy plan submitted to a municipality in accordance with a local emergency energy plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.

(kk) Information and data concerning the distribution of surcharge moneys collected and remitted by wireless carriers under the Wireless Emergency Telephone Safety Act.

(ll) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

(mm) Maps and other records regarding the location or security of a utility's generation, transmission, distribution, storage, gathering, treatment, or switching facilities.

(2) This Section does not authorize withholding of information or limit the availability of records to the public, except as stated in this Section or otherwise provided in this Act.

(Source: P.A. 91-137, eff. 7-16-99; 91-357, eff. 7-29-99; 91-660, eff. 12-22-99; 92-16, eff. 6-28-01; 92-241, eff. 8-3-01; 92-281, eff. 8-7-01; 92-645, eff. 7-11-02; 92-651, eff. 7-11-02.)

Section 99. Effective date. This Act takes effect upon becoming law.

EXHIBIT 15

Everything you need to know about the Cambridge Analytica-Facebook debacle

By **Philip Bump**
Washington Post

MARCH 20, 2018, 7:46 AM

Late on Friday, Facebook made an unexpected announcement: The data firm Cambridge Analytica, hyped as integral to President Donald Trump's election, was suspended from the social network for using data collected improperly from Facebook users.

It is a complicated issue that many people might have missed, given the timing of the announcement. With that in mind, here is an overview of the groups involved, what happened - and what it means.

1. What is Cambridge Analytica?

Cambridge Analytica is a data firm that promises its customers insights into consumer or voter behavior.

On the commercial side, that means tools like "audience segmentation" - breaking out advertising audiences into smaller groups - and then targeting advertisements to those groups on "multiple platforms."

On the political side, it is much the same thing, with one tweak. While advertisers generally target consumers as groups, political campaigns need to target specific people - registered voters receptive to a potential message.

"Combining the precision of data analytics with the insights of behavioral psychology and the best of individually addressable advertising technology," the company's website pledges, "you can run a truly end-to-end campaign." And that is why Cambridge Analytica was created.

Robert Mercer is a prominent conservative donor whose public profile rose sharply over the past few years. He and his daughter Rebekah invested millions in efforts to reshape conservative politics, funding Citizens United, the anti-mainstream-media Media Research Center and Breitbart News.

In 2013, Robert Mercer partnered with a British firm called SCL Group and its elections director Alexander Nix to test SCL's methodology in Virginia's governor's race, as the New York Times reported. Their candidate, Republican Ken Cuccinelli, lost. But the Mercers moved forward with a

political data strategy anyway, partnering with Nix to create Cambridge Analytica, which would use SCL's data and methodology for political work.

2. What prompted the Facebook suspension?

The key part of the Cambridge Analytica sales pitch is that "insights of behavioral psychology" line.

There are lots of data companies that can tell you who's registered to vote, and there are lots of companies that compile consumer data on those same voters. This, in fact, was an instrumental part of Facebook's sales pitch to political campaigns (back before it quietly buried that pitch in the wake of questions about Russian interference in the 2016 election). After the 2014 election, we wrote about how Facebook offered campaigns a place to overlap their voter data (who's registered and basic demographic information) with Facebook's vast array of data on its users' behavior. While most firms that collect data on consumer behavior do so by tracking the bread crumbs we leave around our consumer culture - grocery store rewards cards, magazine subscriptions, etc. - Facebook has the advantage that so many Americans tell the company precisely what they like, by quite literally clicking the "like" button.

Facebook's database of personal information may be the largest in the world, given that nearly a third of the globe has an account with the company. If you are a company looking to provide data services, you would justifiably be jealous of the information Facebook possesses. So Facebook (recognizing an opportunity when it sees it) provides a way for software developers to build on top of their platform, allowing other companies to use their data under certain conditions. It used to be fairly trivial, in fact, for developers to build an application that would then pull a great deal of information from the site, including information about your friends' activity. In May 2014, the site announced it was tightening that access, beginning the following year.

That change came slightly too late.

To apply its "insights of behavioral psychology" to national politics, as the Mercers intended, the SCL/Cambridge team needed a lot of information about a lot of Americans. According to the Times's report, a Cambridge employee named Christopher Wylie encountered a researcher at Cambridge University named Aleksandr Kogan. Kogan built an application that leveraged Facebook's tools to pull information from the site and then pitched its use using Amazon's Mechanical Turk, a tool that allows developers to hire humans (sometimes then referred to as "turkers") to do simple tasks for small fees.

The Intercept reported on how it worked last year.

"The task posted by 'Global Science Research' appeared ordinary, at least on the surface. The company offered turkers $1 or $2 to complete an online survey. But there were a couple of additional requirements as well. First, Global Science Research was only interested in American turkers. Second, the turkers had to download a Facebook app before they could collect payment. Global Science Research said the app would 'download some information about you and your network . . . basic demographics and likes of categories, places, famous people, etc. from you and your friends.' "

Global Science Research was Kogan. Using this method, he gathered information on tens of millions of Americans. (The Times says more than 50 million; other outlets say 30 million.) That information was then used to build out SCL/Cambridge Analytica's profiles.

In building his Facebook application, Kogan had pledged that his data collection was only for research purposes and that it would remain anonymized - not able to be linked to specific people. When the Guardian reported in late 2015 on the link between Kogan and Cambridge, it prompted Facebook to promise to investigate the situation. (The Guardian's story was pegged to Sen. Ted Cruz's (R-Tex.) presidential campaign using Cambridge Analytica for its voter contact efforts. Cruz was strongly supported by the Mercers, who also created well-funded outside groups to promote his candidacy.)

In its statement on Friday announcing the suspensions, Facebook carefully put the blame on Kogan misusing its tools and explained it had demanded in 2015 that Kogan, SCL and Cambridge delete its Facebook data. The suspension was prompted by learning last week - apparently after being contacted by the Times - that Cambridge was still in possession of some of the Facebook data. (The company denies that.)

3. What does Cambridge Analytica's data actually look like?

It is not clear, but we do have one hint.

A professor at New York's New School named David Carroll was studying ad targeting when he realized Cambridge's link with SCL meant the company might be subject to Britain's broader data-access laws, allowing him to potentially see what data the company had collected on him. In March 2017, he got a response that he said "feels roughly accurate."

One can also see how, once the profile was developed, the Facebook data underlying it would become unnecessary. It is as though you sneaked a peek at the secret recipe for Kentucky Fried Chicken and then developed your own recipe based on it. You may not be in possession of the recipe, but that is sort of beside the point.

4. Where does the Trump campaign fit into this?

Trump's digital team was run by Brad Parscale, who last month was named campaign manager for Trump's 2020 effort. Trump's general election campaign was slow to get geared up after the primary, and, by mid-2016, there was a debate over how to invest in digital marketing. Bolstered by Parscale's advocacy (and Jared Kushner's championing) the campaign hired Cambridge Analytica, over then-campaign chairman Paul Manafort's apparent objections. The decision may have been made easier, too, by Cambridge/SCL's role in the successful Brexit campaign in Britain the same month.

As noted above, the Mercers had been hoping Cruz would be the Republican nominee. Once Trump won the Republican nomination, though, they shifted their focus. (The extent to which the hiring of Cambridge Analytica greased that transition is not clear.) They were reportedly instrumental in the August 2016 overhaul of Trump's campaign, recommending the hiring of both Stephen Bannon (from Breitbart) and Kellyanne Conway, who had been working for one of their pro-Cruz PACs.

Over the last few months of the campaign, Parscale's team invested heavily in Facebook advertising, even hosting a Facebook employee at their Texas war room who helped guide their work. The advertising the campaign deployed was informed by Cambridge Analytica's data.

Bloomberg reported on the data team shortly before the election and how Parscale managed the competing data from Cambridge and the Republican Party.

"Parscale was building his own list of Trump supporters, beyond the RNC's reach," Bloomberg's Joshua Green and Sasha Issenberg wrote. "Cambridge Analytica's statistical models isolated likely supporters whom Parscale bombarded with ads on Facebook, while the campaign bought up email lists from the likes of Gingrich and Tea Party groups to prospect for others."

One footnote: Campaign adviser Michael Flynn also contracted with SCL shortly before the end of the campaign, though he apparently never did any work for the company.

5. Does this mean Trump won the election unfairly?

Well, this is a broader question: Does Cambridge help win elections? Or, put another way: How much of Cambridge's rhetoric about psychographics is just hype?

6. Fine. Where has Cambridge Analytica won elections?

In most cases, it is very hard to identify one particular factor that made the difference in a political campaign. Despite the ubiquity of politicking, campaigns do not happen that often and, when they do, there are thousands of factors that make each contest unique. So analyzing the effects of campaign tactics means perusing a small sample in which we are asked to compare apples to oranges to grapes to dogs to stars to love to six.

This is hugely advantageous for political consulting firms because it is often hard to check their claims about how effective they are. Politicians are deeply superstitious and seize on their own and others' past successes to guide their decisions moving forward. What's more, the field of data-driven political persuasion is fairly new, meaning a company that can claim success in a realm many career politicians do not really understand has a huge marketing advantage. Say that you have cracked the code to targeting voters with specific messages, and a lot of campaigns will write you checks.

Cambridge Analytica has not been around that long, but they have been involved in several successful campaigns. There was Sen. Thom Tillis', R-N.C., Senate campaign in 2014, which he won by 1.5 points. There was the "Leave" campaign in the United Kingdom in 2016 which won by 3.8 points. And there was Trump, who lost the popular vote by 2.1 points but won the electoral college.

There were also losing campaigns. Before Trump, the highest-profile effort Cambridge undertook was Cruz's - and he lost. Sure, he ended up in second place in the delegate count despite being fairly unpopular the year before, but his strategy was like Trump's: leverage a core base of support to ride out a crowded field of candidates.

In June 2016, Politico reported that Cruz's team "was disappointed in Cambridge Analytica's services and stopped using them before the Nevada GOP caucuses in late February, according to a former staffer for the Texas Republican."

So it is hard to say in the abstract the effect Cambridge might have had in Trump's race - and it is harder still to say what role the laundered Facebook data played.

Two days before the election, Cambridge's Nix said in an interview that his firm wasn't able to leverage its psychographics on Trump's behalf.

Here is Nix, speaking to TechCrunch:

"We just didn't have the time to rollout that survey. . . . We had to build all the IT, all the infrastructure. There was nothing. There was 30 people on his campaign. Thirty. Even Walker it had 160 (it's probably why he went bust). And he was the first to crash out. So as I've said to other of your [journalist] colleagues, clearly there's psychographic data that's baked-in to legacy models that we built before, because we're not reinventing the wheel. [We've been] using models that are based on models, that are based on models, and we've been building these models for nearly four years. And all of those models had psychographics in them. But did we go out and rollout a long form quantitative psychographics survey specifically for Trump supporters? No. We just didn't have time. We just couldn't do that."

An important asterisk: Two days before the election, Nix (and nearly everyone else in America) likely thought Trump was going to lose. A good way for a political consulting company to cover its back in the event of a loss is to say that it did not have the time to deploy its core value proposition.

7. Is special counsel Robert Mueller III tracking this whole thing?

Apparently.

Given that the Trump campaign and Cambridge invested so much in targeting people online, and given that we know Russian actors tried to leverage Facebook ads and social media to influence voters, there is a natural question as to whether those two efforts had any coordination.

In July, McClatchy reported Mueller's team was looking specifically at that.

"Congressional and Justice Department investigators are focusing on whether Trump's campaign pointed Russian cyber operatives to certain voting jurisdictions in key states," Peter Stone and Greg Gordon wrote. They quoted a former Pentagon staffer named Mike Carpenter. "There appears to have been significant cooperation between Russia's online propaganda machine and individuals in the United States who were knowledgeable about where to target the disinformation," Carpenter said.

8. So are there links to Russia?

Well, it depends on what you mean by "links." We are in this weird moment where any even tangential link to Russia or a Russian person is heralded as a sign of questionable collusion.

So here is what we know.

The Times reports that SCL Group had spoken with the Russian oil giant Lukoil in 2014 and 2015, and that the company "was interested in how data was used to target American voters, according to two former company insiders who said there were at least three meetings with Lukoil executives in London and Turkey." (In an interview with the "Today" show on Monday, Wylie reiterated this claim.)

The paper also notes that Cambridge included questions about Russian President Vladimir Putin in 2014 focus groups, though we will note this was also the time period in which Russia's seizing of Crimea became central to American foreign policy conversations.

Late last year, the Daily Beast reported that Nix had contacted WikiLeaks's Julian Assange before the election offering to host emails stolen from Hillary Clinton's campaign chairman to create a

searchable database. Assange declined the offer. Those emails are believed to have been stolen by Russian hackers linked to the country's intelligence agencies.

One other link is worth mentioning. Kogan, the Cambridge researcher who developed the tool that led to the Facebook suspension, had reportedly also received a grant from the Russian government to research social media.

"Nothing I did on the Russian project was at all related to Cambridge Analytica in any way," Kogan told the Guardian.

This 'attr(data-c-typename)' is related to: Elections, Russia, Donald Trump, Ted Cruz, Robert Mueller III, U.S. Department of Justice, Ken Cuccinelli

Ex. 15-7

EXHIBIT 16

The New York Times

THE SHIFT

Reddit Limits Noxious Content by Giving Trolls Fewer Places to Gather

By Kevin Roose

Sept. 25, 2017

There are — and always have been, and probably always will be — trolls, scoundrels and reprobates on the internet.

It is a problem that has vexed multibillion-dollar corporations and the smartest computer programmers in the world. Facebook, Twitter and YouTube have all declared war on abuse and harassment, spent years training sophisticated algorithms and hired vast armies of moderators to root out hateful content.

And yet, the trolls persist.

But what if a better way of combating online toxicity were right under our noses?

A new study by researchers at Emory University, Georgia Institute of Technology and the University of Michigan suggests that the most effective anti-hate tactic may be what amounts to a nuclear option: identifying and shutting down the spaces where hateful speech occurs, rather than targeting bad actors individually or in groups.

The researchers analyzed 100 million posts originating on two forums on Reddit, the hugely popular online message board. The forums, r/fatpeoplehate and r/CoonTown, were among several that Reddit administrators banned in 2015 as part of a sitewide crackdown on poisonous behavior. (In case the names weren't a tipoff, fatpeoplehate was devoted to photos that mocked overweight people, and CoonTown was filled with racist bile.)

Researchers generated a list of hateful terms used on the two forums, and tracked the use of those terms across Reddit. They also compared the activity of users who posted hateful terms before the bans with those users' activity after, to determine whether they had infiltrated other Reddit forums.

The goal was to figure out what happened when these toxic communities were shut down. Did the amount of hateful language on Reddit decrease? Did users of hateful forums migrate to other parts of the site? Did any of them change their behavior as a result of the bans?

The study found that, to a large extent, the bans worked. Some users who had posted offensive material on the forums that were shut down stopped using Reddit entirely. Of those who continued to use the site, many migrated to other forums, but they did not bring significant amounts of toxic speech with them, and the forums they moved to did not become more hateful as a result of their presence. Over all, the users who stayed on Reddit after the bans took effect decreased their use of hate speech by more than 80 percent.

“By shutting down these echo chambers of hate, Reddit caused the people participating to either leave the site or dramatically change their linguistic behavior,” the researchers wrote.

In an interview, two of the researchers who led the study told me that although they had only examined Reddit, their findings might be applicable to social networks like Facebook and Twitter, which tend to enforce their rules against individuals, rather than groups. They also tend to issue bans in a defensive, case-by-case manner, often in response to user-generated reports of bad behavior.

But the results of the study suggest that proactively shutting down nodes where hateful activity is concentrated may be more effective.

“Banning places where people congregate to engage in certain behaviors makes it harder for them to do so,” said Eshwar Chandrasekharan, a doctoral student at Georgia Tech and the study’s lead author.

Eric Gilbert, an associate professor at the University of Michigan and one of the researchers involved in the study, said that Reddit’s approach worked because it had a clear set of targets. “They didn’t ban people,” he said. “They didn’t ban words. They banned the spaces where those words were likely to be written down.”

This is, of course, a small case study — two Reddit forums out of millions of online spaces where antisocial behavior occurs — and methods for quantifying hate speech are still imperfect. (This study’s approach would have flagged one user chastising another for using a racist slur as hateful speech, if the slur were repeated as part of the chastising, for example.) The study also did not account for users who left Reddit altogether, some of whom may have continued to use hate speech elsewhere online.

Other online communities have had success with a broad-based approach to moderating hate speech. Discord, a private chat app, banned several large right-wing political chat rooms from its platform this year, after some of the speech turned hateful and violent. The bans did not entirely end hate speech on Discord, but they did break up these communities and made it harder for trolls to find and talk with one another.

There is no guarantee that a similar approach would work on a larger network. And there are risks to employing aggressive moderation tactics. Some platforms, such as YouTube, have been criticized when their hate speech filters have wrongly targeted videos posted by lesbian, gay, bisexual and transgender creators. Twitter's banning of a number of alt-right activists en masse last year prompted a right-wing backlash. And Facebook's security chief, who said last month that the social network shut down more than a million accounts every day, has also said that policing hate speech more aggressively would increase the number of "false positives," or posts wrongly flagged as offensive.

Social networks are increasingly feeling pressure to address hateful speech, not just for the sake of users but in response to legal and political challenges. German authorities, for example, have threatened to fine social networks, including Facebook and Twitter, up to 50 million euros, or $53 million, for failing to remove harmful content in a timely manner.

As these platforms strategize about how to take on hate speech, it would be smart to study the geography of their networks — which groups, pages and subcommunities tend to encourage this behavior — and the effect of closing those spaces, even without a specific violation or report of abusive speech.

It might seem odd to focus on a space, rather than on a person or an act. But as the Reddit example shows, the broadest approach is sometimes the right one.

Correction: Sept. 25, 2017
An earlier version of the picture caption with this article referred incorrectly to Alexis Ohanian's role at Reddit. He is a founder of the site, not the chairman.

Follow Kevin Roose on Twitter @kevinroose.

EXHIBIT 17

DATAMINR IN THE NEWS

Share:

Article: Dataminr announces new tool to assist first responders

May 16, 2017 | TechCrunch | Dataminr introduced a new product on stage at TechCrunch Disrupt in New York City that searches the Twitter firehose for emergency situations throughout the city, and channels news alerts to first responders.

READ IN TECHCRUNCH

VIEW ALL PRESS

VIEW ALL RESOURCES

Official Partner Dataminr is an Official Twitter Partner

$

SOLUTIONS

- Corporate Security
- Finance
- Public Sector
- News
- PR / Communications

RESOURCES

- All Resources
- Case Studies
- Articles
- Infographics
- Reports
- Videos
- Webinars

ABOUT

- About Dataminr
- Team
- Careers
- Events
- Press
- FAQ
- Contact Us

SUBSCRIBE TO THE DEBRIEF NEWSLETTER

Gain monthly insights into how Dataminr alerts clients to breaking events in real time.

WORK EMAIL *

SOLUTION:

CORPORATE SECURITY

SUBSCRIBE

Welcome! Are you ready to learn about the value of real-time information?

4