In The
Supreme Court of Virginia

Record No. 170247

Harrison Neal,
Appellant,

v.

Fairfax County Police Department, et al.,
Appellees.

Brief of Digital Recognition Network, Inc. &
Vigilant Solutions, Inc.
As *Amici Curiae* In Support of Appellees

Michael A. Carvin
(*Pro hac vice* pending)
Ryan J. Watson
(*Pro hac vice* pending)
Andrew Bentz (VSB No. 84860)
Counsel of Record
JONES DAY
51 Louisiana Ave., N.W.
Washington, D.C. 20001
Tel: (202) 879-3849
Fax: (202) 626-1700
abentz@jonesday.com

Counsel for Amici Curiae *Digital Recognition Network, Inc.*
& Vigilant Solutions, Inc.

SCV: Submitted on 08-25-2017 14:21:26 EDT for filing on 08-25-2017

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTRODUCTION 1

INTEREST OF *AMICI CURIAE* 1

STATEMENT OF THE CASE 2

STATEMENT OF THE FACTS 3

STANDARD OF REVIEW 4

ARGUMENT 4

I. ALPR INFORMATION IS NOT PERSONAL INFORMATION 4

II. ALPR USE IS NOT ANALOGOUS TO GPS TRACKING OR CELL PHONE LOCATION DATA 9

III. LICENSE-PLATE NUMBERS ARE NOT "AGENCY-ISSUED IDENTIFICATION NUMBERS." 12

IV. FCPD IS COVERED BY THE DATA ACT'S CRIMINAL INVESTIGATION EXEMPTION 14

CONCLUSION 16

CERTIFICATE OF COMPLIANCE AND SERVICE

TABLE OF AUTHORITIES

Page(s)

CASES

ACLU v. Clapper,
959 F. Supp. 2d 724 (S.D.N.Y. 2013) 12

Conyers v. Martial Arts World of Richmond, Inc.,
273 Va. 96 (2007) 4

In re App. of the United States for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013) 11

Maracich v. Spears,
133 S. Ct. 2191 (2013).....14

New York v. Class,
475 U.S. 106 (1986).....5, 6

Olabisiomotosho v. City of Houston,
185 F.3d 521 (5th Cir. 1999) 6

People v. Weaver,
909 N.E.2d 1195 (N.Y. 2009).....10

Riley v. California,
134 S. Ct. 2473 (2014).....11

Smith v. Maryland,
442 U.S. 735 (1979).....6

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) 11

United States v. Davis,
785 F.3d 498 (11th Cir.) (en banc) 10, 11, 12

United States v. Diaz-Castaneda,
494 F.3d 1146 (9th Cir. 2007) 6

United States v. Ellison,
462 F.3d 557 (6th Cir. 2006) 6

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) (en banc) 11

United States v. Jones,
565 U.S. 400 (2012).....10, 11

United States v. Knotts,
460 U.S. 276 (1983).....7

United States v. Miranda–Sotolongo,
827 F.3d 663 (7th Cir. 2016) 6

United States v. Sparks,
37 F. App'x 826 (8th Cir. 2002) (unpublished).....6

United States v. Sparks,
750 F. Supp. 2d 384 (D. Mass. 2010).....12

United States v. Walraven,
892 F.2d 972 (10th Cir. 1989) 6

United States v. Wilcox,
415 F. App'x 990 (11th Cir. 2011) (per curiam) (unpublished).....6

Wooley v. Maynard,
430 U.S. 705 (1977).....5

STATUTES

18 U.S.C. § 2721 14

Va. Code Ann. § 2.2-3800 1

Va. Code Ann. § 2.2-3801 13

Va. Code Ann. § 2.2-3802 14

Va. Code Ann. § 2.2-3803 7

Va. Code Ann. § 46.2-711 5

Va. Code Ann. § 46.2-715 5

Va. Code Ann. § 46.2-716 5

INTRODUCTION

Appellant Harrison Neal alleges that certain aspects of the Fairfax County Police Department's ("FCPD") use of Automated License Plate Readers ("ALPRs") to collect, store, search, and disseminate license-plate information violate Virginia's Government Data Collection and Dissemination Practices Act, which regulates collection, storage, use, and dissemination of "personal information" by government agencies. Va. Code § 2.2-3800 *et seq*. As the Circuit Court found, "[t]here is one salient issue that this Court must decide: is a license plate number personal information?" Decision Below at 1. The answer to that question is a resounding "no": ALPR information plainly is not "personal information." And "[o]nce the issue of whether a license plate is personal information is decided in the negative, there is no material issue of fact and the analysis need go no further." *Id.* at 6. Accordingly, this Court should affirm the Circuit Court's decision.

INTEREST OF *AMICI CURIAE*

Digital Recognition Network, Inc. ("DRN") and Vigilant Solutions, Inc. ("Vigilant") perform work relating to ALPRs. DRN uses photographs and image-content analysis techniques to serve the financial services, insurance, and vehicle repossession industries. DRN and others use such techniques in an effort to locate specific content within a photograph—namely, the alphanumeric content printed on a license plate. DRN's ALPR systems, which are typically mounted on tow

trucks, take photographs that include nearby vehicles' license plates. Software cross-checks the alphanumeric characters from the license plates against a database of license plates that are registered to vehicles that are sought for recovery by one of DRN's clients. DRN then disseminates the resulting license-plate data to its clients and partners, which use the data for purposes such as identifying cars that should be repossessed and locating cars that have been stolen or fraudulently reported as stolen.

DRN also provides captured license-plate data to Vigilant, which then shares the data with law enforcement agencies. Such agencies then use the data for purposes that range from utilizing near real-time alerts for locating missing persons and stolen vehicles to the use of historical license-plate data to solve crimes.

The issue in this case—whether license-plate data is "personal information"—is important to both DRN's and Vigilant's businesses. Indeed, the Fairfax County Circuit Court granted DRN and Vigilant amicus status in the proceeding below. Given their extensive experience with the technology implicated in this case, DRN and Vigilant offer this brief to aid the Court's consideration of this case.

STATEMENT OF THE CASE

On May 5, 2015, Neal filed a complaint in Fairfax County Circuit Court seeking to prevent FCPD from so-called "passive use" of ALPR data—i.e., the

collection of "unanalyzed [ALPR] data for potential future use." Br. of Appellant 6 ("Neal Br."); JA 1-28.[1] FCPD demurred, asserting that the ALPR data it stores and uses do not fall within the statutory definition of "personal information" under the Data Act. JA 37-38, 45-67. On August 28, 2015, Judge Grace Burke Carroll denied FCPD's demurrer. JA 464.

The case proceeded to discovery, after which both Neal and FCPD moved for summary judgment. Neal Br. 2. Fairfax Circuit Court Judge Robert Smith held that ALPR records are not "personal information" and therefore granted FCPD summary judgment. JA 782-87. The court entered a final order on November 22, 2016 (JA 788-89), and Neal filed a timely Notice of Appeal. This Court granted Neal's petition to appeal on June 22, 2017.

STATEMENT OF THE FACTS

FCPD uses ALPR devices and databases in its efforts to provide safety for the citizens of Fairfax County. An ALPR system photographs license plates and records the time the photograph is taken and the location of the ALPR system and camera. JA 782-87. The device can be stationary or attached to vehicles. *Id.* The information gathered by ALPRs is stored in a searchable digital format, and FCPD stores this data for up to one year. JA 15. Neal's license plate was photographed

[1] In contrast, Neal does not challenge "active use" of ALPR data, which involves the collection and real-time analysis of ALPR data to assess its relevance to "'an ongoing case or emergency.'" Neal Br. 6.

on two occasions by one of FCPD's ALPRs and stored in FCPD's ALPR system. JA 719-720. Neal claims FCPD's "passive" collection, use, and storage of ALPR data violates the Data Act, which protects "personal information."

STANDARD OF REVIEW

"[A]n issue of statutory interpretation is a pure question of law which [the Court] review[s] de novo." *Conyers v. Martial Arts World of Richmond, Inc.*, 273 Va. 96, 104 (2007).[2]

ARGUMENT

I. ALPR INFORMATION IS NOT PERSONAL INFORMATION.

License plates contain no sensitive or private information whatsoever. Indeed, *none* of the information that ALPR systems typically collect—a license-plate photograph, as well as the date, time, and location of the camera—contains personally identifiable information such as the owner's name or address. The court below explained that it is "undisputed" in this case that the FCPD's database "did not contain Neal's name, address, date of birth or any information related to the registered owner of the vehicle." Decision Below at 2–3. In short, Neal's concern that ALPR data will be used to create a "dossier" about him is counter-factual and

[2] Neal's brief lists two "assignments of error"—namely, that the court below (1) *should not* have granted FCPD's summary judgment motion and (2) *should* have granted Neal's summary judgment motion. The appellate standard of review, as well as the relevant facts and legal arguments discussed in the present amicus brief, apply to both assignments of error.

far-fetched. Neal Br. 36.

As a threshold and dispositive matter, license plate numbers are plainly not "personal information" whose use and dissemination are limited in order to deter public disclosure of private facts. To the contrary, the entire purpose of license plate numbers is to *publicly display* information for vehicle identification purposes. Specifically, a license plate is essentially a "mobile billboard," *see Wooley v. Maynard*, 430 U.S. 705, 715 (1977), that is seen by countless others whenever a vehicle is in public view. A license-plate number is a government-mandated mechanism for *public* identification, which is why license plates must be displayed on the front and rear of cars in a "clearly visible" and "clearly legible" manner. Va. Code §§ 46.2-711, 46.2-715, 46.2-716. A license plate's function is to identify a vehicle, so that other private actors (*e.g.*, witnesses to an accident) or public entities (*e.g.*, police) can ascertain where the vehicle was and when it was there, thus facilitating imposition of damages or penalties on the vehicle's driver or owner (which is often times not the same individual).

In a case involving a vehicle identification number—located *inside* a car but typically viewable from *outside* it—the Supreme Court held that "it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile." *New York v. Class*, 475 U.S. 106, 114 (1986). Numerous courts have applied this

reasoning to license plates, which are likewise "required by law to be located in a place ordinarily in plain view from the exterior of the automobile." *Id.* In fact, at least seven federal courts of appeals have concluded that there is not a privacy interest in license plates. *United States v. Miranda–Sotolongo*, 827 F.3d 663, 667-68 (7th Cir. 2016); *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151, 1153 (9th Cir. 2007); *United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006); *Olabisiomotosho v. City of Houston*, 185 F.3d 521, 529 (5th Cir. 1999) ("A motorist has no privacy interest in her license plate number."); *United States v. Walraven*, 892 F.2d 972, 974 (10th Cir. 1989) ("[B]ecause they are in plain view, no privacy interest exists in license plates."); *United States v. Wilcox*, 415 F. App'x 990, 991–92 (11th Cir. 2011) (per curiam) (unpublished); *United States v. Sparks*, 37 F. App'x 826, 829 (8th Cir. 2002) (unpublished).

Moreover, when individuals drive on a public street (or park in a public place), they obviously are choosing to publicly convey information about the vehicle's whereabouts, which can be observed by anyone. It is well established that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). In fact, Neal concedes that "what one chooses to display openly is *not* within the ambit of Fourth Amendment 'privacy.'" Neal Br. 32 n.16 (emphasis added). Thus, there is no reasonable expectation of privacy in information about

the location of a vehicle that is being driven in a public place. Indeed, decades ago, the Supreme Court held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *United States v. Knotts*, 460 U.S. 276, 281 (1983).

Neal's position also has absurd implications. Since Neal contends that ALPR data is personal information subject to the Data Act, which severely limits dissemination of that information, then he presumably believes that police cannot disseminate a photograph of a license plate to investigate crime. *See* VA Code § 2.2-3803(1).[3] Under that view, for example, the police could not show the photo to victims and ask if that was the car that ran them over.

It is true that Neal is not challenging what he has termed "active" use, which is supposedly distinct from "passive" use. Neal's distinction seems to be that the police can start collecting and using ALPR data *after* a crime is committed, but not before. Neal Br. 6. This distinction is found nowhere in the Data Act and makes no practical sense. As a statutory matter, Neal's brief to this Court does not explain why his argument that ALPR data is personal information would not equally apply to "active" use of ALPR data. ALPR data is either personal information under the Data Act or it is not. Its character as personal information

[3] Although the statute does permit dissemination for a "proper agency purpose," VA Code § 2.2-3803(1), it is far from clear that Neal would consider this use of ALPR data to be proper.

does not turn on the use of the information. Neither does its character transform from non-personal to personal because the information is stored for potential use in a future investigation. Moreover, as a practical matter, permitting police to collect information only after crimes are committed would make investigations vastly more difficult and costly. Often when a person commits a crime, he flees the area. It is thus imperative to have information on who or what was in the area before or when the crime was committed. But under Neal's theory, police cannot store ALPR data until after they get the 911 call. Such a hamstrung investigation is clearly not what the legislature intended.

In short, it is not remotely conceivable that the General Assembly thought license-plate information was "*personal* information," to be protected from public disclosure, given that the Assembly *required* that such information be displayed to the *public*. (And, of course, license plate information is not "*personal*" information since it only identifies the *vehicle*. *See infra* pp. 12-13). Nor can it coherently be maintained that the photographic *recording* of government-mandated license plates infringes some privacy interest that concededly is not infringed when the photographer *views* the plate. Since the government commands that the plate be divulged to *all* people in a position to view it, the additional act of recording what everyone can see entails no invasion of privacy distinct from this universal viewing. In short, because there is no privacy interest in the underlying data that

are displayed to the entire public, there cannot rationally be a privacy interest that precludes the recording or storing of that data.[4]

II. ALPR USE IS NOT ANALOGOUS TO GPS TRACKING OR CELL PHONE LOCATION DATA.

In arguing that ALPR information is "personal information," Neal and his amicus attempt to analogize ALPR systems to GPS monitoring or cell phone location data. Neal Br. 11; Amicus Br. of Electronic Frontier Foundation in Support of Appellant 8, 15–17 ("EFF Br."); *see also* Neal Br. in Opp'n to Demurrer 5–6 ("Opp'n"); Amicus Br. of Electronic Frontier Foundation in Support of Petition for Review 16. In their view, the police can use ALPR systems to compile information about a person's movements, in a way that could reveal information about medical appointments, attendance at worship services, and the like. But ALPR information is not analogous to location data from GPS trackers or cell phones.

First, unlike data culled from a GPS device or a cell phone, license-plate information cannot be used to continuously track a car or an individual. License-plate data are merely snapshots of a vehicle's location at isolated points in time, not a 24/7 stream of data about a person's whereabouts. This distinction is starkly

[4] Even if certain ALPR systems incidentally capture information such as "weather conditions" or "traffic" (Neal Br. 23, 29), such information is obviously not "personal information." Otherwise the Virginia statute would regulate weather cameras and the like.

demonstrated by the fact that this case involves ALPR data captured about a particular vehicle on a grand total of *two* occasions (Neal Br. 7–8), not a constant stream of tracking information such as that produced by a GPS tracker. *See People v. Weaver*, 909 N.E.2d 1195, 1195–96, 1202–03 (N.Y. 2009) ("constant[]" GPS monitoring "for 65 days"). It is, therefore, perfectly clear that ALPR data are *not* "just as revealing" (EFF Br. 17) as GPS tracking.

Second, even if license-plate information captured by an ALPR system could hypothetically somehow be used to conduct constant surveillance, it is, at best, an extraordinarily inefficient means of doing so. Once a vehicle has been identified for surveillance because it is associated with a crime, why would officers follow that vehicle with an ALPR system that continually notifies them that the vehicle they are following is associated with a crime? Law-enforcement officers bent on constantly tracking someone's movements would not likely use ALPR data for this purpose; rather, they would use far more direct surveillance methods.

Third, the U.S. Supreme Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), is plainly inapposite here. The majority opinion in *Jones* was based on a "trespass" theory of the Fourth Amendment, which is unquestionably inapplicable here because ALPR systems do not physically intrude on a constitutionally protected area. *See id.* at 405 & 406 n.3, 412; *United States v. Davis*, 785 F.3d 498, 513–14 (11th Cir.) (en banc) (emphasizing that *Jones* relied

on a physical-trespass theory), *cert. denied*, 136 S. Ct. 479 (2015) (mem.). Moreover, even Justice Alito's separate opinion expressed privacy concerns only about certain "longer term GPS monitoring," 565 U.S. at 430 (Alito, J., concurring in the judgment)—and, as noted, ALPR data cannot realistically be used for such long-term, continuous surveillance.

Fourth, the ACLU has acknowledged that "tracking" based on cell phone information is "more detailed and invasive" than so-called "tracking" based on vehicle locations. *In re App. of the United States for Historical Cell Site Data*, 724 F.3d 600, 609 (5th Cir. 2013); *see generally Riley v. California*, 134 S. Ct. 2473, 2490 (2014). This is a significant concession, given that many courts have concluded that even the acquisition of historical cell phone location data or telephone metadata does not violate the Fourth Amendment. *United States v. Graham*, 824 F.3d 421, 427 (4th Cir. 2016) (en banc) (no "reasonable expectation of privacy in the historical [cell-site location information]"); *Davis*, 785 F.3d at 511, 513–14; *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).[5]

---

[5] The United States Supreme Court recently granted certiorari to decide "[w]hether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment." Pet. for Writ of Cert. i, *Carpenter*, 137 S. Ct. 2211 (No. 16-402), 2016 WL 5462796 (filed Sept. 26, 2016). Petitioner in that case emphasizes that the State seized nearly four months' worth of location

(continued)

Fifth, a privacy interest is not implicated simply because a significant amount of license-plate data may be aggregated in a database. Numerous courts have recognized that non-private data are not transformed into private data simply because there is a substantial amount of data. *See Davis*, 785 F.3d at 515; *ACLU v. Clapper*, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013), *aff'd in part, vacated in part by* 785 F.3d 787 (2d Cir. 2015); *United States v. Sparks*, 750 F. Supp. 2d 384, 395–96 (D. Mass. 2010), *aff'd*, 711 F.3d 58 (1st Cir. 2013). Simply put, since photographing one picture of a license plate with a normal camera does not invade privacy or record "personal information," photographing numerous license plates through ALPR does not either.

III. LICENSE-PLATE NUMBERS ARE NOT "AGENCY-ISSUED IDENTIFICATION NUMBERS."

Neal also contends that ALPR information is "personal information" because that term includes "agency-issued identification number[s]" and, in his view, a license-plate number is an "agency-issued identification number." Neal Br. 24-28. Not so. As relevant here, "[p]ersonal information" includes "all information that … describes, locates or indexes *anything about an individual* including, but not limited to, his social security number, driver's license number,

(continued…)
data, and that "people carry their phones with them virtually everywhere they go, including inside their homes and other constitutionally protected spaces." Pet. i, 29. Such concerns are not even remotely implicated by the FCPD's use of license-plate data.

agency-issued identification number, … medical history, … or employment record." Va. Code § 2.2-3801 (emphasis added). The italicized text—"anything about an individual"—makes clear that the word "identification" refers to "identification" of a person, not a vehicle. *See* Decision Below at 5 ("All the information included in the statute refers to an individual person."). This is also underscored by the definition's other examples, such as social security numbers and medical history, which plainly refer to individuals. Importantly, however, a license plate identifies a vehicle—not a person. The plate reflects the fact that the vehicle has been registered with the Department of Motor Vehicles and is authorized to be used on the roads, but it does not identify anything about a person. For that reason, a license plate is not an "agency-issued identification number[]" under the statute.

Finally, Neal previously contended that if a license-plate number is typed into the database maintained by the Department of Motor Vehicles, it can be linked to an individual's name and personal data. *See* Opp'n 6–7; *see generally* Neal Br. 4. This argument fails to demonstrate that a license-plate number is "personal" information. As an initial matter, the federal Drivers Privacy Protection Act ("DPPA") "establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent"; thus, insofar as a person obtains such information about a driver, it is because he had a legally permissible purpose to request the information (or the driver voluntarily disclosed

it). *Maracich v. Spears*, 133 S. Ct. 2191, 2198 (2013) (internal quotation marks omitted) (citing 18 U.S.C. §§ 2721(a)(l), (a)(2)). And although the DPPA provides an exception for law enforcement agencies, *see* § 2721(b)(1), it is important to note that, "[b]y referring to other databases[,] the license plate number can lead the researcher to the owner of the vehicle *and nothing more*." Decision Below at 5 (emphasis added). For example, "[a] license plate number does not tell the researcher where the person is, what the person is doing, or anything else about the person." *Id.* In any event, even if *public* information (such as a license-plate number) could be used to obtain access to "personal" information, that would not magically transform the public information into "personal" information.

IV. FCPD IS COVERED BY THE DATA ACT'S CRIMINAL INVESTIGATION EXEMPTION.

Even if—contrary to normal English, the law, and numerous court decisions holding that license plates are not private—ALPR data is personal information under the Data Act, Neal's case fails for a wholly separate reason. The Data Act specifically exempts from its coverage "information systems" that "deal with investigations and intelligence gathering relating to criminal activity." Va. Code Ann. § 2.2-3802(7). There can be no doubt that FCPD's information systems in which the ALPR data are stored serve investigations and intelligence gathering related to criminal activity. If there were any doubt, the evidence in the record dispels it. FCPD has used the ALPR database to investigate murders, robberies,

and assaults, as well as to locate fugitives and recover stolen vehicles. *See* Opp'n to Pet. for Appeal 15.

Neal attempts to draw a distinction between "passive" and "active" collection. He appears to believe that police can collect ALPR data after a crime has been committed ("active"), but police cannot collect ALPR data before a crime is committed ("passive"). But, as noted above, this purported distinction does not save his position. *See supra* pp. 7-8. This distinction is found nowhere in the statute; either ALPR data is personal information or it is not. *See id.* Neal's distinction also makes no sense: Surely a storeowner does not wait to turn on a security camera until *after* a crime has been committed, in the hopes of capturing an image of the suspect if he is dumb enough to re-enter the store at a future date. Likewise, the police should not be required to wait to use ALPR systems until after a vehicle has been used in the commission of a crime.

In any event, FCPD's so-called "passive" collection and maintenance of ALPR data *is* plainly for investigative purposes, as ample record evidence demonstrates. *See* Opp'n to Pet. for Appeal 15-16. FCPD's collection and use of ALPR data is thus exempt from the Data Act.

CONCLUSION

This Court should affirm.

Dated: August 25, 2017

Respectfully submitted,

/s/ Andrew Bentz

Michael A. Carvin
(*Pro hac vice* pending)
Ryan J. Watson
(*Pro hac vice* pending)
Andrew Bentz (VSB No. 84860)
Counsel of Record
JONES DAY
51 Louisiana Ave., N.W.
Washington, D.C. 20001
Tel: (202) 879-3849
Fax: (202) 626-1700
abentz@jonesday.com

CERTIFICATE OF SERVICE AND COMPLIANCE

I certify that on August 25, 2017, three printed copies were hand-delivered to the Clerk of this Court and an electronic copy was filed via VACES. An electronic copy was served, via email, upon:

Edward S. Rosenthal
Jessica R. Killeen
RICH ROSENTHAL BRINCEFIELD MANITTA
DZUBIN & KROEGER, LLP
201 North Union Street, Suite 230
Alexandria, Virginia 22314
ESRosenthal@RRBMDK.com
JRKilleen@RRBMDK.com

Elizabeth D. Teare
Karen L. Gibbons
Kimberly P. Baucom
Senior Assistant County Attorney
OFFICE OF THE COUNTY ATTORNEY
12000 Government Ctr. Pkwy, Suite 549
Fairfax, Virginia 22030
elizabeth.teare@fairfaxcounty.gov
karen.gibbons@fairfaxcounty.gov
kimberly.baucom@fairfaxcounty.gov

Leslie C. Mehta
Hope R. Amezquita
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, INC.
701 East Franklin Street, Suite 1412
Richmond, Virginia 23219
lmehta@acluva.org
hamezquita@acluva.org

Matthew J. Erausquin
CONSUMER LITIGATION ASSOCIATES, P.C.
1800 Diagonal Road, Suite 600
Alexandria, VA 22314
matt@clalegal.com

I also certify the foregoing does not exceed 50 pages and that it complies with Rules 5:26 and 5:30 of the Rules of the Supreme Court of Virginia.

Dated: August 25, 2017

*/s/ Andrew Bentz*_____
Andrew Bentz
Counsel for Amici Curiae *Digital Recognition Network, Inc. & Vigilant Solutions, Inc.*