

VIRGINIA:

IN THE CIRCUIT COURT OF THE COUNTY OF FAIRFAX

HARRISON NEAL,)
)
 Plaintiff,)
)
 v.)
)
 FAIRFAX COUNTY POLICE)
 DEPARTMENT, et al.,)
 Defendants.)
 _____)

Case No. CL-2015-5902

PLAINTIFF HARRISON NEAL'S CLOSING ARGUMENT BRIEF

Edward S. Rosenthal (VSB No. 15780)
Lana M. Manitta (VSB No. 42994)
Jennifer A. Lucey (VSB No. 83603)
RICH ROSENTHAL BRINCEFIELD MANITTA
DZUBIN & KROEGER, PLLC
500 Montgomery Street, Suite 600
Alexandria, Virginia 22314
(703) 299-3440 phone
(703) 299-3441 fax
Email: ESRosenthal@RRBMDK.com
Email: LMManitta@RRBMDK.com
Email: JALucey@RRBMDK.com
Counsel for Harrison Neal, Plaintiff

I. INTRODUCTION

This case will determine whether the automatic license plate reader (“ALPR”) program used by Defendant Fairfax County Police Department (hereinafter “FCPD”)—a program that the Supreme Court of Virginia referred to as a “sweeping randomized surveillance and collection of personal information”¹—is governed by the Virginia Government Data Collection and Dissemination Practices Act (“Data Act”),² or instead, by rules and limitations solely of Defendants’ own choosing. At stake are the security and privacy of untold thousands of “images of [a] vehicle, its licenseplate, and the vehicle’s immediate surroundings, along with the GPS location, time, and date when the image was captured,”³ collected by the ALPR technology (“ALPR data”), which are stored and searchable at a moment’s notice at the discretion of any among scores of sworn and civilian employees of FCPD who have access to the system. The capture and long-term storage of ALPR data on motorists driving in Fairfax County in the hope that this trove might be useful to some hypothetical future FCPD investigation is referred to as the “passive use” of ALPRs. Upon remand from the Supreme Court, this case now turns on whether “the *total components and operations of the ALPR record-keeping process* provide a means through which a link between a license plate number and the vehicle’s owner may be readily made.” *Neal*, 295 Va. at 348, 350.

As emphasized repeatedly in FCPD’s own operating protocols and training materials,⁴ the ultimate purpose of ALPR technology is to solve crimes: to identify suspects, to locate witnesses, and to make arrests.⁵ Defendants claim that their passive use of ALPR data is of inestimable value to each

¹ *Neal v. Fairfax Cty. Police Dep’t.*, 295 Va. 334, 349 (2018).

² The name of the Act was changed in 2001 from the “Privacy Protection Act of 1976” to the “Government Data Collection and Dissemination Practices Act”.

³ *Neal*, 295 Va. at 346.

⁴ FCPD’s Standard Operating Procedure 11-039 (“SOP”) and “e-learning course and past power point presentations” are the authoritative “written policy, rule or practice of FCPD ... relating to the collection, storage, access, use, and/or dissemination of information collected using ALPR technology.” Trial, Pt. 1 (“TR1”) 25:10-20 (reading PX 84, INT 3).

⁵ *E.g.*, TR1 38: 19–39: 5 (reading PX 87, RFA 1); DX 5, Sec. VI.O.; PX 30, 1:52-2:43, 10:58-11:48; PX 32, p. Defendants’ Document Production, Bates #000454 (“B# 454”), B# 468; PX 33, p. B# 3077, B# 3084; PX 34, p. B# 337.

of these objectives, a vital “investigative tool to aid in the detection or investigation of terrorism or a series of related crimes.” *See e.g.*, DX 5, Sec. VI.O. At the most intuitive level, for such an “investigative tool” to be effective, it must ultimately lead to a criminal, *i.e.*, a *person*. Accordingly, as Judge Carroll observed in overruling FCPD’s demurrer, the program “is an information system as well with the data points and components and operations of a record keeping process. Otherwise, what would be the point of holding that information?” *Order 8/28/15*.⁶

II. ISSUE ON REMAND

On appeal from this Court, the Supreme Court observed that “an agency’s ‘record-keeping process’ is an ‘information system’ if it contains both ‘personal information and the name, personal number, or other identifying particulars’ of an individual.” *Neal*, 295 Va. at 347. The Supreme Court held, *inter alia*, that “in the context of the DMV database, a license plate number, such as ‘ADDCAR,’ is an agency-issued number that identifies the owner of the vehicle, in this case Neal.” *Id.* at 345-46. The court held that “the pictures and data associated with each license plate number constitute ‘personal information’ as defined by Code § 2.2-3801.” *Id.* at 346. The court went on to state:

Here, as explained above, the Police Department’s “passive use” of its ALPRs, including the ALPR database, is a “record-keeping process” that includes data that contains “personal information,” in that the ALPR database captures and stores images of the vehicle, as well as the time, date, and GPS location when the images were captured. Thus, the determination of whether the ALPR database is an “information system” under the Data Act turns on whether it also contains “the name, personal number, or other identifying particulars” of an individual.

[A] license plate number may be an “identifying particular” because it has the potential to identify the individual to whom the plate number is registered in the same way a “name” or “personal number” identifies the individual to which it is assigned.

Id. at 347-48. Upon review of the record of the cross-motions for summary judgment, the Supreme Court found insufficient evidence of the specific components and operations of the ALPR system or

⁶ The quotation is from the Hearing Transcript of 8/28/2015, 32:1-4, which was incorporated into the Order.

of any DMV connection to make such a determination:

In the present case, however, it remains to be seen whether a sufficient link can be drawn to qualify a license plate number as an “identifying particular.” Although the *ALPR database* does not contain any information related to the individual to whom a specific license plate number is registered, that does not mean that the *total components of the Police Department’s ALPR record-keeping process* do not provide a means for discerning that information. On the record before this Court, however, we cannot say whether or not such a means exists as part of the ALPR record-keeping process. Accordingly, we will remand the matter to the circuit court for a determination of whether *the total components and operations of the ALPR record-keeping process* provide a means through which a link between a license plate number and the vehicle's owner may be readily made.

Id. at 348 (emphasis added). Accordingly, this Court’s task is to examine the entirety of the ALPR record-keeping process—not just the ALPR database—to determine whether it “provide[s] a means through which a link between a license plate number and the vehicle’s owner may be readily made.”

Id. If any means exist through which such a link may be readily made, then FCPD’s use of ALPRs is subject to the Data Act, and Neal is entitled to judgment.⁷ Conversely, only if the Court concludes that no means exist by which such a link may be readily made is a judgment for FCPD warranted.

III. THE EVIDENCE

ALPR technology uses cameras, working with computer software, to detect and capture images of license plates of cars coming within the range of the ALPR cameras.⁸ FCPD uses ALPR cameras affixed to the exterior of police cruisers and to stationary units or trailers. DX 6; TR1 47:22–43:5. Cameras affixed to a police cruiser can capture 5-7,000 license plate reads during an 8-hour shift.⁹

When an ALPR camera detects a license plate, it takes pictures of the tag, which include, at a minimum, color and infrared images of the car on which the plate is located and its surroundings. *Neal*, 295 Va. at 346-47; PX 30, 7:49-7:51; PX 32, p. B# 462. *See also, e.g.*, PX 12. A built-in GPS

⁷ The Supreme Court noted FCPD’s concession that if the Data Act is applicable to their passive use of ALPRs, then their current policy is in violation of the Data Act and Neal is entitled to judgment. *Neal*, 295 Va. at 342.

⁸ DX 5, Sec. IV.; PX 30 4:27-4:40; PX. 32, pp. B# 457-58; PX 34, p. B# 339.

⁹ PX 34, p. B# 338; PX 30 6:29-6:44; PX 32, B# 460.

capability records and stamps the precise geospatial coordinates, date, and time the pictures were captured.¹⁰ All this information constitutes the “ALPR data” associated with that particular license plate and vehicle. *Neal*, 295 Va. at 346-47. The software scans and converts the images of the license to searchable alphanumeric characters. PX. 34, B# 339. The captured GPS data and images are stored in a dedicated database, and they may be retrieved by tag number, time, or location.¹¹

FPCPD receives a “hot list” of suspect tag numbers made available by the Virginia State Police, twice each day, downloaded automatically, through a direct computer link, without human intervention by anyone at FPCPD. DX 5, Sec. V.B.; TR2 226:17–227:11. A qualified ALPR user can also add a new, local “hot” tag number in their vehicle. PX 30, 25:35-26:01; PX 32, p. B# 519. The “hot list” generally consists of license numbers “that are associated with some type of criminal activity or police interest,” TR2 166:21–167:1., *e.g.*, with stolen vehicles, wanted suspects, missing persons, abductions or Amber Alerts.¹² If a plate scanned matches a plate on the hot list, the program will notify the user that a license plate associated with the hot list has been detected.¹³ If there is no match, the data remains in the ALPR database for up to 365 days, where it can be queried, examined, and used to aid a theoretical future investigation.¹⁴ For purposes of such “passive use” of ALPR data, the SOP requires that all ALPR records—including the vast majority of them, like Neal’s vehicle, with no connection whatsoever to any crime or investigation—

will be maintained on the server for a period not to exceed 365 days without specific authorization of the Chief of Police. The purpose of the retention period is to increase protection of the community by providing an investigative tool to aid in the detection or investigation of terrorism or series of related crimes.

¹⁰ DX 5, Sec. IV.; PX 30, 10:30-10:57; PX 32, pp. B# 467-468, B# 531-533. *See, e.g.*, PX 12.

¹¹ DX 5, Secs. VI.C., VI.O., X.; TR1 109:11–110:15; PX 30, 27:56-28:16, 28:50-29:21, 31:01-31:50; PX 32, p. B# 519, 525, 528-29, 533, 543. *See also, e.g.*, PX 12; Trial Transcript, Day 2, (“TR2”) 207:20-210:8.

¹² PX 30, 1:52-2:43, 10:58-11:48; PX 32, p. B# 454, 468, 519; PX 33, p. B# 3077, 3084; PX 34, p. B# 337, 357.

¹³ DX 5, Sec. IV.; PX 30 4:50-5:12; PX 32, pp. B# 458-59, 501, 504; PX 34, pp. B# 356-59.

¹⁴ DX 5, Sec. VI.C., Sec. VI.O.; TR1 38:19-39:5 (reading PX 87, RFA 1); TR1 109:11–110:15.

DX 5, Sec. VI.O. By Defendants' own admission, such "passive use" of ALPR data is for investigative purposes, and Defendants consider *every vehicle* to be a *potential lead, i.e., a target*:

The use of crime-fighting technology such as LPR is necessary to develop investigative leads. LPR uses a force multiplier reducing the ability of vehicles related to law enforcement events to slip through staffing gaps. *All vehicles on the public roadways* in Fairfax County represent *potential investigative leads* when considering the 447,818 calls for services FCPD responded to in 2014.

TR1 38:19-39:5 (reading PX 87, RFA 1) (emphasis added).

ALPR-trained crime analysts and sworn officers have access to the ALPR database through Mobile Computer Terminals ("MCTs") in police cruisers, MCTs or "CADs" (for Computer Aided Dispatch) and/or stationary office computers. DX 5, Secs. IV, VI.C., VI.O. Mobile and stationary computers enable ALPR-qualified users to search, retrieve, and inspect previously-captured ALPR data records by tag number, time, and location.¹⁵ The SOP requires that ALPR-qualified crime analysts and officers have "full access" to all entries in the ALPR database: "Crime analysts and sworn employees trained in the use of the ELSAG Operations Center software shall have *full access* to ALPR data *to conduct analysis of data and processing requests for data* from any Police Department employee having a legitimate law enforcement request." DX 5, Sec. VI.C. (emphasis added). FCPD's training materials are used to teach ALPR users specifically how ALPR data collected during a shift *can be used* to help identify a suspect.¹⁶ Maj. Hurlock, Director of the ALPR program, acknowledged that Defendants' ALPR data can also be an investigative tool to identify a witness. TR1 118:8-14.

At the same time, FCPD MCTs and desktop computers provide entrée to powerful law

¹⁵ DX 5, Secs. VI.C., VI.O., X.; TR1 109:11-110:15; PX 30, 27:56-28:16, 28:50-29:21, 31:01-31:50; PX 32, p. B# 519, 525, 528-29, 533, 543. *See also, e.g.*, PX 12; TR2 207:20-210:8.

¹⁶ *See e.g.*, PX 30, 1:52-2:43, 10:58-11:48; PX 32, p. B# 454, 468.

enforcement data such as those found in the VCIN/DMV/NCIC networks.¹⁷ These database applications are not locally stored or automatically connected; but it is beyond dispute that they are *readily accessible*, in some cases on the same terminals that access stored ALPR data. As a local Virginia criminal justice agency, *see* Va. Code § 9.1-101, FCPD participates in these networks, and their authorized employees enjoy ready access to them. Tr. 164, Ln. 19-22.¹⁸ In discovery on remand, Defendants made conclusive admissions (*see* Va. Sup. Ct. R. 4:1(b)) as to their ready access to all information generally—and motor vehicle ownership and driver data in particular—in the DMV, VCIN, and NCIC law enforcement networks to which they belong:

[I]n police vehicles equipped with ALPR technology, *the same mobile computing device on which the ALPR program resides* also contains one or more programs capable of accessing *DMV registration data, VCIN criminal information, and NCIC criminal information* pertaining to motor vehicles and their *owners and operators*.

TR1 40:3-10 (reading PX 92, RFA 6) (emphasis added). Defendants' sworn interrogatory responses detail the simple steps an officer uses to obtain ownership information as to any tag of interest:

Once an officer has a license plate number, the officer enters the number into the computer aided dispatch (CAD) terminal in the police vehicle. Once the officer hits "Enter," multiple queries are performed by the computer including queries to the DMV, VCIN, and I/LEAD's databases. The return *provides the identity [of the] registered owner* of the vehicle associated with the license plate number. Also included is the *information that is contained on the registration card* issued to the owner.

¹⁷ The primary law enforcement data networks are the National Criminal Information Center (NCIC), hosted by the FBI (TR2 163:18-164:3); the Virginia Crime Information Network (VCIN), made available to in-state law enforcement by the Virginia State Police (TR2 164:4-10); and the Virginia Department of Motor Vehicles (DMV) (TR2 164:11-18). We will refer to these three VSP-centered networks as "VCIN/DMV". *See* TR2 164:19-22; TR1 40:3-10 (reading PX 92, RFA 6); TR1 41:22-42:17 (reading PX 92, Interrogatory ("INT") 3); TR1 42:18-43:5 (reading PX 92, INT 4).

¹⁸ Under Va. Code § 46.2-208(9), virtually unfettered access to these otherwise "privileged" DMV records is open to any law enforcement officer "in order to carry out [his] official functions". "On the request of any ... law-enforcement officer ... the Commissioner shall (i) ... provide the ... law-enforcement officer ... with correct information as contained in the Department's records and (ii) provide driver and vehicle information in the form of an abstract of the record showing all convictions, accidents, driver's license suspensions or revocations, and other appropriate information as the ... law-enforcement officer ... may require in order to carry out [his] official functions." *Id.* Va. Code § 19.2-389 provides similar access to criminal justice data through the VCIN and NCIC networks by all "[a]uthorized officers or employees of criminal justice agencies, as defined by § 9.1-101, for purposes of the administration of criminal justice."

TR1 41:22–42:17 (reading PX 92, INT 3) (emphasis added). An officer or crime analyst in an office location would go through these same steps, using a fixed computer workstation as opposed to a mobile CAD terminal. TR1 42:18-43:5 (reading PX 92, INT 4). Defendants formally admitted that “FCPD officers and crime analysts can *readily access motor vehicle registration information* with respect to any vehicle registered in the Commonwealth of Virginia *by inquiring by telephone or otherwise with Virginia DMV.*” TR1 41:15-21 (reading PX 92, RFA 8) (emphasis added).

Lt. Rex Pagerie’s testimony confirms the ready means by which the networked VCIN/DMV databases are accessed. With the MCT, an officer would turn on the MCT and log in with her ID, after which (a minute or two), the officer would then be able to access both the ALPR program and the I/Mobile program. TR2 183:14-22. The VCIN/DMV databases are accessed by simply logging in to the I/Mobile platform (clicking an icon and entering user credentials), waiting for authentication, and then clicking on a tab within the I/Mobile platform that allows the user to query *all three* databases at once. TR2 184:1–185:16. Lt. Pagerie acknowledged that officers generally already have the MCTs up and running while on duty in a cruiser. TR2 223:1-8. Indeed, the MCT *must* be on for the ALPR technology to operate.¹⁹ Thus, practically speaking, a user need do no more than close or minimize the ALPR program, log in to I/Mobile, click on a tab, and she can easily query the entire set of VCIN/DMV databases. This VCIN/DMV network, though accessed manually, allows direct and immediate access to law enforcement and motor vehicle information and other identifying particulars.

Undisputed evidence establishes that FCPD’s ALPR SOP itself requires uses of these same networked databases. SOP 11-039, DX 5, lays out the many components and operations that comprise FCPD’s use of its ALPR tools. In using ALPR data to pursue an investigation or work a lead, users must verify the accuracy of the information contained in the captured ALPR record: “An FCPD

¹⁹ PX 30, 8:40-9:20; 16:40-18:08; 33:01-34:20; PX 32, pp. B# 464-467, 474-475, 479, 496.

officer who has the authority to use the LPR system would ascertain that the information provided in the LPR database was current and accurate prior to taking law enforcement action or otherwise using the data provided.” TR1 51:3-8 (reading PX 87, RFA 3). Before use of ALPR data to further an investigation, the data must be verified and leveraged; something that is done by query to DMV and/or links to the VCIN/DMV networks via applications on an MCT or desktop computer.²⁰ The SOP and training materials make clear that verification of ALPR data through the VCIN/DMV law enforcement networks is a necessary precondition before “making a stop or effecting an arrest” on that basis.²¹ “Once a visual comparison is confirmed, the operator shall verify the hit is still active by running the information via MCT or voice a request for a NCIC/VCIN through DPSC.” *Id.* at Sec. VI.I.2. Moreover, the SOP requires that, “All contacts resulting from ALPR use shall be documented as appropriate in the I/Leads Records Management System” or by “using the COMMENT button from the event screen in I/Mobile.” *Id.* at Sec. VI.M. *See also* TR2 195:1–196:10.

On two separate occasions FCPD captured and stored for a full year Neal’s personal information showing images of the vehicle owned by and registered to Neal, his vanity license plate (ADDCAR), the car’s immediate surroundings, and its GPS location, time and date. PX 12. Neal testified that he himself was driving his automobile on both of those occasions, and that he is the primary owner and user of that automobile. TR1 87:7-88:18. FCPD’s written responses to Neal’s inquiries are examples of the ready retrieval of ALPR data from the ALPR database by a crime analyst. PX 12. In this case, contrary to Defendants’ protestations that the database is accessed only for specific law enforcement purposes, this “passive use” and dissemination of Neal’s ALPR data clearly had no law enforcement “investigative purpose.” (*See* testimony of Lt. Palenscar, stating FCPD provides ALPR data on a

²⁰ *See* TR141:22–42:17 (reading PX 92, INT 3); TR1 42:18–43:5 (reading PX 92, INT 4).

²¹ DX 5, Sec. VI.I.; PX 30, 19:13-19:21, 22:48-23:42; PX 32, p. B# 501, 512; PX 34, p. B# 358-59.

requested tag number to anyone making a FOIA request. TR1 104:5-11).

IV. ARGUMENT

The Data Act defines an “information system” as “the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.” Va. Code § 2.2-3801. The question for this Court is whether FCPD’s ALPR record-keeping process constitutes an “information system”, *i.e.*, whether “the total components and operations of [the ALPR] record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual”, Va. Code § 2.2-3801, “provide a means through which a link between a license plate number and the vehicle’s owner may be readily made.” *Neal*, 295 Va. 348. The evidence establishes that such a link may be readily made through routine use of the VCIN/DMV network in conjunction with ALPR technology. Undisputed evidence, indeed Defendants’ conclusive admissions, establish that, using the requisite broad and liberal reading and application of the Data Act and the Supreme Court’s opinion, the vehicular ownership information readily available to FCPD officials through their participation in the VCIN/DMV networks provides the means through which a link satisfying the elements of an information system may readily be made.

A. The Data Act Is A Remedial Statute, And All Elements Of The “Information System” Must Be Liberally Construed

1. The Data Act, All of Its Terms, and The Evidence Must be Liberally Construed and Applied to Fulfill the Legislature’s Remedial Purposes

“[T]he [Data] Act ‘is an important initial step towards safeguarding Virginia citizens against abusive information-gathering practices.’” *Hinderliter v. Humphries*, 224 Va. 439, 443 (1982), (quoting 62 Va. L. Rev. 1357, 1358 (1976)). In ordering a remand, the Supreme Court placed great

emphasis on the “remedial purposes” of the Data Act and the necessity of a broad construction:

[The Act] expressly declares its remedial purpose is to “preserve the rights guaranteed a citizen in a free society” by “establish[ing] procedures to govern information systems containing records on individuals.” . . . Notably, the General Assembly includes in the statute specific findings, including that “[a]n individual’s privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;” “sophisticated information technology has greatly magnified the harm that can occur from these practices;” “[a]n individual’s opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems;” and “legislation is necessary to establish procedures to govern information systems containing records on individuals.” Further . . . [the Act] provides a mechanism for relief to “[a]ny aggrieved person” by which that person “may institute a proceeding for injunction or mandamus *against any person or agency* that has engaged, is engaged, or is about to engage *in any acts or practices in violation* of the provisions of this chapter.”

“Every statute is to be read so as to promote the ability of the enactment to remedy the mischief at which it is directed.” Remedial statutes are to be liberally construed “so as to suppress the mischief and advance the remedy in accordance with the legislature’s intended purpose.” “All other rules of construction are subservient to that intent.” *Id.*

Neal, 295 Va. at 344 (internal citations omitted; emphasis added) (quoting Va. Code §§ 2.2-3800(B)(1)-(4), 3809; *Bd. of Supervisors of King and Queen Cty. v. King Land Corp.*, 238 Va. 97, 103 (1989); *Univ. of Va. v. Harris*, 239 Va. 119, 124 (1990)). The protections of the Data Act apply only to “information systems.” Therefore, just as the Supreme Court applied a liberal construction of the Data Act and the evidence in holding ALPR data constituted “personal information,”²² the term “information system” under the Data Act and evidence regarding an “information system” must be liberally construed to fulfill the legislature’s remedial purposes in enacting the Data Act.

2. None of the Words of the Statute May Be Ignored

A Virginia court “must ... assume that the legislature chose, with care, the words it used when

²² “The conclusion that the picture and associated data is ‘personal information’ is consistent with the legislature’s intent to remedy the potential mischief posed by ‘the extensive collection, maintenance, use and dissemination of personal information’ and the potential for misuse of such information. Code § 2.2-3800(B)(1); *see University of Virginia*, 239 Va. at 124, 387 S.E.2d at 775.” *Neal*, 295 Va. at 347.

it enacted the relevant statute, and we are bound by those words as we interpret the statute.” *Barr v. Town & Country Prop., Inc.*, 240 Va. 292, 295 (1990). “The manifest intention of the legislature, clearly disclosed by its language, must be applied. There can be no departure from the words used where the intention is clear.” *Id.* (quoting *Anderson v. Commw.*, 182 Va. 560, 566 (1944)). No part of a statute may be rendered meaningless unless absolutely unavoidable. *Garrison v. First Fed. Savings*, 241 Va. 335, 340 (1991); *Northampton Cty. Bd. of Zoning App. v. E. Shore Dev. Corp.*, 277 Va. 198, 202 (2009). When different terms appear in the same section, the terms are presumed to have a different meaning from one another. *Klarfeld v. Salisbury*, 233 Va. 277, 284-85 (1987).

It is within this context that the ordinary meaning of the key terms of both the statute and the Supreme Court’s remand directive must be applied. Critical statutory words such as “total”, “components and operations”, “process”, “automated or manual”, “collected or managed”, “computer networks”, “identifying” and “identifiable particulars”, may not be disregarded, ignored, or read so narrowly as to deprive them of effect. And the same must be said for the language of potentiality (e.g., “potential mischief”, “potential for misuse”, “potential to identify”, “provide a means for discerning”, “a means through which a link ... may be readily made”) carefully chosen by the Supreme Court in its twice-repeated remand directive. Cf. *Neal*, 295 Va. at 348, 350. Scrupulously adhering to the import of these words, to a plain understanding of the intentions behind them, and to the salient facts Defendants have admitted on remand about the particulars of their links to the VCIN/DMV network should lead to the unavoidable conclusion that the VCIN/DMV network link is an integral part of the complex and many-sided “information system” for maintaining, organizing, and using data pertaining to FCPD’s ALPR technology.

3. The History of the Data Act Also Demands A Broad Construction

Plaintiff’s expert, Professor Neil Richards, provided testimony regarding the historical context

in which the General Assembly enacted the Data Act. As he explained,

The Data Act was passed at a time of tremendous uncertainty and anxiety about privacy in American society at all levels. ... In the 1960s the computer technologies that had first been deployed during the Second World War for good and for evil began to bear fruit ... as these technologies began to be deployed by corporations and by governments, the use of computers, the use of databanks, the use of linking of databanks together, American society, both at a popular level and at the level of law at the federal and state level began to address these issues.

TR2 79:11-80:11. Discussions of privacy and data security began to appear in popular culture. *See*

TR2 80:12-14. Watergate caused anxiety about recording, surveillance, and privacy. TR2 82:16-83:1.

The U.S. Supreme Court issued a series of opinions “declaring privacy to be protected in various ways by the Constitution and federal statutes.” TR2 80:19-21. The U.S. Dept. of Health, Education, and Welfare empaneled a commission “to study the problem of databanks and of linkage and of the privacy harms that emerge from government use of personal information in the computer context, the collection, the use, the dissemination, the disclosure, the retention” (“Ware Commission”). TR2 81:17-82:3. The Ware Commission’s 1973 report established the “Fair Information Practices Principles” for data processing (“FIPPs”). TR2 82:4-15. The FIPPs include principles such as “that notice is given of data processing; that some meaningful choice is given, particularly if information that’s collected for one purpose is used for another; requirements of access and rectification for data subjects; requirements of security.” TR2 86:16-21. *See e.g.*, Virginia Code § 22-3800(C). Laws protecting information and privacy, including the Freedom of Information Act and the Privacy Act, were enacted. TR2 81:6-14.

In this environment, in 1976, the General Assembly enacted the Data Act after first “commissioning the VALC, the Virginia Advisory Legislative Council, to study the problem of databases and personal information, computer processing.” TR2 83:2-11. The VALC recommended

the protection of privacy as a fundamental right. TR2 83:11-17.²³ “[T]he creation of dossiers on individuals that can follow them around”, “linkage of databases that have personal information”, and “the increasing use of computers and sophisticated information technology” were found to have “magnified the harm that can occur from these practices.” TR2 94:2-22. The FIPPs were incorporated into the Data Act. TR2 83:18-84:9; 87:2-14. Code § 22-3800(B) expressly highlights how the “increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from [data processing].” TR2 86:3-5. The Data Act is intended to endure as a remedial statute “to deal with new kinds of processing, new kinds of computers, new kinds of data collection” (TR2 96:1-11), and it was specifically intended to be construed liberally.

B. The “Total Components and Operations” Of FCPD’s Record-Keeping Process Include Not Only Local ALPR Data, Software, And Equipment, But All Elements And Uses Applied To Leverage Stored ALPR Data For Investigative Purposes

1. “The total components and operations”

According to Merriam-Webster, “*total*” means, “comprising or constituting a whole.”²⁴ It is synonymous with “whole” “entire” and “all,” and means “including everything or everyone without exception,” and implies “that nothing has been omitted, ignored, abated, or taken away.” *Id.* “*Component*” means “a constituent part: ingredient,”²⁵ and it is synonymous with a building block, element, factor, or member. “*Operation*” means “performance of a practical work or of something involving the practical application of principles or processes.”²⁶ The ordinary meaning of the phrase “*total components and operations*” is thus the *entire collection of constituent parts, including all of the elements and processes.*

²³ See also *Hinderliter v. Humphries*, 224 Va. 439, 442-49 (1982) for a discussion regarding the legislative history.

²⁴ *Total*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/total> (Feb. 1, 2019). (Dates in citations to websites are the last-visited date).

²⁵ *Component*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/component> (Jan. 29, 2019).

²⁶ *Operation*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/operation> (Jan. 29, 2019).

The total components and operations of FCPD's passive use of ALPRs includes *all elements, processes, and uses* related to collecting ALPR data and leveraging ALPR data for investigative leads, including those referred to in the SOP and Defendants' training materials. FCPD's own Standard Operating Procedure 11-039, identifies the purpose of the SOP as "to establish specific procedures pertaining to the operating guidelines, maintenance, data retention, storage, access, release of information, and the responsibilities relevant to the use and operation of Automatic License Plate Readers (ALPR) and associated data." DX 5, Sec. I. Defendants would have the Court simply ignore *some* of the express components and operations included in their own ALPR operating manual. For example, FCPD's ALPR SOP contains three distinct references to the use of the VCIN/DMV network. First, the "hot list" automatically loaded into the FCPD ALPR system twice each day comes directly to the ALPR server by virtue of its automated connection to the VSP VCIN/DMV network. *Id.*, Sec. V.B. SOP Section VI.I affirmatively requires the use of the VCIN/DMV network by an ALPR user to verify a "hit" on a vehicle whose information has been captured by ALPR technology. *Id.*, Sec. VI.I. *See also id.* at Section VI.I.2 ("Once a visual comparison is confirmed, the operator shall verify the hit is still active by running the information via MCT or voice a request for a NCIC/VCIN through DPSC.")²⁷ SOP Section VI.J. requires that "license plate responses from NCIC/VCIN shall be confirmed by Teletype in accordance with established procedures as soon as practical." *Id.*

SOP Sec. VI. calls for an elaborate, multi-layered process by which investigative leads developed using ALPR data must be documented. Defendants' arguments about the scope of their ALPR program do not account for these intricate additional record-keeping processes; they treat all

²⁷ Defendants refer to this procedure in their sworn answer to interrogatories: "An FCPD officer who has the authority to use the LPR system would ascertain that the information provided in the LPR database was current and accurate prior to taking law enforcement action or otherwise using the data provided." TR1 51:3-8 (reading PX 87; RFA 3).

practices pursuant to these follow-up protocols as if they do not exist. Furthermore, SOP Section VI.M. makes clear that FCPD's ALPR record-keeping process is *itself* but one component of FCPD's comprehensive I/LEADS "Records Management System": "All contacts resulting from ALPR use shall be documented as appropriate in the I/Leads Records Management System" or by "using the COMMENT button from the event screen in I/Mobile." DX 5, Sec. VI.M.; *see also* TR2 195:1–196:10. After completing a manual entry for a new license plate of interest, the investigating officer is obliged to "query the ALPR data to determine if the license plate was scanned previously." *Id.*, Sec. VI.L. Whenever investigative information has "evidentiary value," the SOP requires "downloading of the applicable data from the ALPR server onto a CD-R for filing," to be stored in the FCPD's "Record Room" as well as "one additional copy for [the officer's] case file." *Id.*, Sec. VI.L. If information has "evidentiary value," the SOP requires "downloading of the applicable data from the ALPR server onto a CD-R for filing," to be stored in the FCPD's "Record Room" as well as "one additional copy for [the officer's] case file." *Id.*, Secs. VI.D-VI.F. Article VII of the SOP provides a similarly broad and extensive set of secondary (*i.e.*, external to the data housed on FCPD's ALPR server) record-keeping requirements and protocols for ALPR data that is shared with outside law enforcement agencies. *Id.*, Secs. VII.A.-VII.E. "At the discretion of the ALPR operator, additional information may be entered into the ALPR System at any time." *See id.*, Sec. VI.K.

Since FCPD's SOP expressly requires ALPR users to employ law enforcement networks (*e.g.*, VCIN/DMV) and comprehensive record-keeping applications (*e.g.*, as catalogued in SOP Articles VI and VII, FCPD's I/LEADS or I/Mobile record-keeping programs, CD-Rs, case files, notes and comments), those same networks, applications, documents, and activities must be considered to belong among the "total components and operations" comprising the entire ALPR record-keeping process. In determining the scope of the entire FCPD ALPR process, there is no justification for

ignoring, as FCPD would have it, tools used and information collected, managed, or acted upon in investigative steps, procedures, and documentation regarding vehicles of interest stored in the ALPR database. These potential and actual investigative uses and/or misuses of ALPR-captured personal information evidencing vehicular travel indisputably are part of the total components and operations of the ALPR record-keeping process.

Viewing these tools in practical terms demonstrates that the scope of the ALPR record-keeping process is best seen to be as wide as *all* of FCPD's operations, procedures, and components for the collection, recordation, and use of ALPR law enforcement data. At a minimum, since the link to the VCIN/DMV network made available through the VSP is one of the technical tools, steps, and actions expressly called for in FCPD's ALPR SOP, it must be, by definition, among the "*components and operations*" of that "*total*" "record-keeping *process*." Accordingly, the SOP definitively establishes FCPD's admitted use of its connection to the VCIN/DMV network as precisely the potential "*link*" that the Supreme Court tasked the parties and this Court to flesh out between FCPD's stored ALPR data on "ADDCAR" and DMV's records revealing Neal's ownership of that vehicle.

2. "of a record-keeping process"

The choice by the legislature to use—and by the Supreme Court to stress—the term "process" has great significance in determining the parameters of FCPD's passive use of ALPR technology. "*Process*" can have many meanings, but the most pertinent one here is "a series of actions or operations conducing to an end."²⁸ The "*end*" of the FCPD ALPR process is not just to collect and store thousands of GPS travel records for 365 days at a time. Defendants' own admissions conclusively establish that the ALPR record-keeping process is far more than just a database of license plate numbers; the software that manages the database; and the equipment on which it is

²⁸ *Process*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/process> (Jan. 29, 2019).

accessed. The ALPR tool is best seen as an investigative gateway to the movements, whereabouts, and ultimately, the identity of vehicles, suspects, witnesses, and other persons of interest to police:

The use of crime-fighting technology such as LPR is necessary to develop investigative leads. LPR uses a force multiplier reducing the ability of vehicles related to law enforcement events to slip through staffing gaps. *All vehicles on the public roadways* in Fairfax County *represent potential investigative leads* when considering the 447,818 calls for services FCPD responded to in 2014.

TR1 38:19-39:5 (reading PX 87, RFA 1) (emphasis added).

FCPD's own SOP and training materials make abundantly clear that the ultimate purpose of the program is to collect and store license plate information in a way that is readily useable for responding to investigative leads, locating persons of interest, identifying suspects, and making arrests.²⁹ Those underlying purposes require moving from vehicles to owners, drivers, and occupants. The quickest, simplest, and most effective way of doing that is through the readily accessible link that FCPD employees use each day to "run the tag number" through VCIN/DMV.

As the definitions above underscore, the FCPD's ALPR "record-keeping process" includes every step, component, element, tool, and operation involved in the actual and potential passive use of ALPR technology, including any investigative leads or activities capable of leveraging captured ALPR data to identify, locate, and develop suspects and witnesses, to solve crimes, and to lead to arrests and convictions.

3. "collected or managed by means of computer networks or the Internet"

Among the many meanings of "*network*" in the context of computers is "a system of computers and peripherals that are able to communicate with each other."³⁰ Defendants contend the VCIN/DMV networks to which they belong—*networks* specifically identified and invoked in their SOP—should

²⁹ DX 5, Sec. II., Sec. VI.O.; PX 30, 1:52-2:43, 10:58-11:48; PX 32, p. B# 454, 468, 519; PX 33, p. B# 3077, 3084; PX 34, p. B# 337.

³⁰ *Network*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/network> (Jan. 29, 2019).

somehow not be counted as part of the *total components and operations* of their own ALPR program. Ostensibly, their rationale is based on the premise that the data they access and share through those networks are not hosted locally by FCPD. This contention fails to take into account that part of FCPD's own ALPR "record-keeping process" involves, indisputably, (a) downloaded information – *e.g.*, the twice-daily VCIN/DMV "hot lists" that FCPD *collects, manages, stores, incorporates,* and *uses* upon receipt from VSP (DX 5, Sec. V.B.; TR2 226:17–227:11); (b) specific data that FCPD ALPR users are required to verify by affirmatively querying, receiving, and comparing before taking law enforcement action whenever they have a "hit" on a suspect vehicle in the ALPR database (DX 5, Secs. VI.I., VI.I.2., VI.J.); and (c) follow-up information the SOP requires to be documented in FCPD's own comprehensive Records Management System, I/LEADS (or I/Mobile), with respect to any investigative leads developed from ALPR records (DX 5, Sec. VI.M.; TR2 195:1–196:10).³¹

The fact that those networks are hosted by another agency is not controlling; the key point is that FCPD enjoys unrestricted, direct, and immediate access to the data available through those networks. What is important is that these networks *provide a "means"* through which FCPD personnel can "*readily*" make the connection between a captured tag number in its ALPR database and the DMV record from which to discern the identity of the owner and likely driver of the vehicle. That was the test posited by the Supreme Court, and it is that test on which we must focus. The inescapable facts are that (a) FCPD participates and shares in the VCIN/DMV networks, (b) its ALPR users have direct, immediate access to these networks, *see e.g.*, Va. Code § 19.2-389 and Va. Code § 46.2-208(9), and (c) the ALPR SOP makes the use of this link *mandatory* in the development and verification of investigative leads relating to captured ALPR records. FCPD's actual and potential

³¹ The results of investigative inquiries—for verification or otherwise—made using the VCIN/DMV networks for motor vehicle ownership information are clearly "collected" by those "computer networks." Documenting those results in the I/LEADS or I/Mobile record system, as required by the SOP Section VI.M., plainly involves stored ALPR-related information being "managed" by another component or operation of the total ALPR record-keeping process.

access to the VCIN/DMV computer network³² belongs among the integral “total components and operations” of FCPD’s ALPR record-keeping process.

4. “whether automated or manual”

“*Automated*” means “operated automatically,”³³ while “*manual*” means “of, relating to, or involving the hands; worked or done by hand and not by machine; requiring or using physical skill and energy”.³⁴ Defendants’ contend that the actual and potential links to the VCIN/DMV networks should not be considered part of FCPD’s ALPR record-keeping process because their use, despite being readily available at the touch of a mouse or keyboard, requires individual investigative action by a law enforcement actor and are not a routine or automatic part of the ALPR protocol. This argument should be soundly rejected.

First, the “hot list” link between the ALPR server and the VCIN/DMV network is direct, immediate, and *automatic*, and it takes place twice each day. DX 5, Sec. V.B.; TR2 226:17–227:11. This undisputed evidence establishes that there is indeed an *automated* link between these two databases. Second, Defendants’ admissions conclusively establish that through a variety of unfettered *manual* connections, FCPD ALPR-qualified personnel can and do readily seek and obtain vehicle ownership information pertaining to any vehicle of interest, including vehicles that have been captured and stored in FCPD’s ALPR database. Information that identifies the owner of any Virginia-registered vehicle is available in a matter of seconds or minutes, using a few keystrokes on the same MCT unit deployed in ALPR-equipped cruisers or one of many office computers from which ALPR

³² The statute’s inclusion of connections through “the Internet”, though not dispositive here, is nevertheless highly instructive. If the “total components and operations” of a record-keeping process that is “collected or managed by means of ... the Internet, whether automated or manual...” comprise a single “information system”, the breadth of the Data Act is almost limitless. The Internet has become so enormous a repository of readily searchable data that few subjects cannot be searched, collected, and used there. Surely, if the legislature intended the Data Act to apply to the nearly infinite data that may be collected and managed over the Internet, making FCPD responsible to obey the Act’s rules and limits for information readily obtainable through law enforcement networks it belongs to is a trifling imposition.

³³ *Automated*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/automated> (Jan. 29, 2019).

³⁴ *Manual*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/manual> (Jan. 29, 2019).

users (when not in such a cruiser) may connect with the VCIN/DMV networks. This simple, fast, and convenient *network* connection may not qualify as “*automated*,” but that is not the proper test. The ability to run an ALPR-stored tag through the DMV/VCIN networks via FCPD computers/terminals, dispatchers, crime analysts, or authorized ALPR users, meets the Virginia Supreme Court’s test as “*manual*” “*means*” through which FCPD can and does “*collect*” and “*manage*” a “*link*” between captured ALPR data and VSP-hosted ownership data that identifies the vehicle’s owner. To find otherwise would be reading the term “*manual*”³⁵ right out of the Data Act.

C. FCPD’s Passive Use of ALPRs Provides A Means Through Which A Link May Be Readily Made Between A License Plate And A Vehicle’s Registered Owner

Although FCPD is correct that the *ALPR database* does not in and of itself identify Neal by name, the Supreme Court expressly ruled that this fact does not preclude a finding that the “*total components and operations of the ALPR record-keeping process*” includes a link through which such identification may be “*readily made*.” *Neal*, 295 Va. at 348. As the Supreme Court observed, the Data Act makes the presence of a social security number, a name, or an analogous “*identifying particular*” enough to complete an “*information system*” because it provides the “*potential to identify*” the individual to which it is assigned. *Id.* That “*potential*” is the capacity of that name or number to serve as a “*link*” or gateway to what might be an external, but readily accessible, source. In the context of the FCPD ALPR surveillance system, that link is FCPD’s direct, simple, and immediate access to VCIN/DMV law enforcement networks.

FCPD admitted that its ALPR-qualified FCPD crime analysts and sworn officers enjoy nearly instantaneous access to the VCIN/DMV network, some of them on the same MCTs that also control

³⁵ “A widely available business textbook points out that “*people*” and “*process*” are key components of an “*information system*.” Dave Bourgeois & David T. Bourgeois, *Information Systems for Business and Beyond*, Ch. 1 (2014), <https://bus206.pressbooks.com/chapter/chapter-1>.

their entrée to the ALPR database.³⁶ See, e.g., TR1 41:22–42:17 (reading PX 92, INT 3) (“[T]he officer enters the number into the computer aided dispatch (CAD) terminal in the police vehicle. Once the officer hits ‘Enter,’ multiple queries are performed by the computer including queries to the DMV, VCIN, and I/LEAD’s databases.”) Other ALPR users can quickly log on to those networks on office workstations doing the same. TR1 42:18–43:5 (reading PX 92, INT 4). Indeed, the testimony of Lt. Pagerie buttressed these admissions. He established that officers generally have their MCTs running while on duty in a cruiser. TR2 223:1-8.³⁷ Once the MCT is “on”, the VCIN/DMV databases are accessed by clicking an icon to log in to the I/Mobile platform, entering the user’s credentials, and clicking on a tab within the platform that allows the user to query *all three* databases at once. TR2 184:1-185:16. A telephone call to DMV provides another simple, direct, and immediate means for establishing the link between an ALPR-captured tag number and a wealth of detailed information regarding the owner and likely driver associated with that tag. TR1 41:15-21 (reading PX 92, RFA 8). Even an officer without direct personal qualifications to use the ALPR program can establish the same link between a captured ALPR data record and the identity of its owner and likely driver by requesting the assistance of a dispatcher, crime analyst, officer, or administrator with qualifications. DX 5, Sec. VI.C; (TR1 41:15-21 (reading PX 92, RFA 8)). By virtue of Defendants’ own formal admissions, see Rule 4:11(b), plus the above-cited evidence at trial, Neal has proven that the VCIN/DMV networks, part of the total ALPR record-keeping process, provide a means by which a link between an ALPR-captured tag number and its owner (and probable driver) can be *readily made*.

D. “Potential” Uses and Misuses of FCPD’s ALPR Technology

As the Supreme Court held, and Professor Richards’ testimony emphasized, the legislature

³⁶ See TR1 164:21-166:11; TR1 40:3-10 (reading PX 92, RFA 6); TR1 41:22–42:17 (reading PX 92, INT 3).

³⁷ Again, the MCTs must be on for the ALPR technology to operate. PX 30, 8:40-9:20; 16:40-18:08; 33:01-34:20; PX 32, pp. B# 464-467, 474-475, 479, 496.

wanted the prophylactic standards, guidelines, and limitations of the Data Act to provide safeguards to make overuse, misuse, compromise, or unnecessary disclosure of personal information, like Neal’s travel activities, less likely. They did that through a robust, coordinated, and balanced set of rules and regulations intended to apply—with certain well-defined and narrow exceptions not relevant here—to all readily identifiable personal information collected and stored by the government. In view of this statutory purpose, it is simply not for FCPD to say that its own different set of rules and regulations—changeable at will—is a substitute for the safeguards the Virginia General Assembly enacted. The fact that FCPD can point to some other law, regulation, or ethical precept that it has adopted that might reduce or deter some of the misuse—if ever discovered, investigated, or enforced—is irrelevant. For example, just because there are laws against stealing does not mean that no other precautions or safeguards are needed to make that prospect less likely to occur. In view of this overarching legislative purpose, as Professor Richards explained, the emphasis in the wording of the statutory definitions and in the language used in the opinion of the Supreme Court on *potential* as well as *actual* uses and misuses is striking.

At the same time, Defendants seem to argue that their program of massive collection and storage of motorists’ personal information does not constitute an “information system,” unless Neal can find and elicit proof that the readily available “links” between the ALPR vehicle data and the VCIN/DMV data that would identify the vehicle’s owner and likely driver have *regularly* been used and *misused*. This contention misperceives the remedial purposes of the Data Act and the focus, both in the statutory language and in the Supreme Court’s opinion in *Neal*, on the idea of the potential³⁸ for misuse of the system’s capabilities, and the value of strong, comprehensive, and uniform state-

³⁸ “Potential” is defined as “existing in possibility”, “capable of development into actuality”, or “expressing possibility.” *Potential*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/potential> (Jan. 29, 2019).

wide procedural barriers against the realization of such hazards. In addition to the express language of the Data Act itself, we call the Court’s attention to the persistent emphasis by the Supreme Court on phrases reflecting capabilities (as opposed to manifestations): “*the potential mischief posed*,” *Neal* 295 Va. at 347; “*the potential for misuse*,” *id.*; “*is indexed or may be located*,” *id.*, “*other identifiable*³⁹ *particulars*,” *id.*; “*other identifying particulars*,” *id.*⁴⁰; “*has the potential to identify*,”⁴¹ *id.* at 348; “*provide a means for discerning*,”⁴² *id.*; “*whether or not such a means exists*,” *id.*; and “*a means through which a link between a license plate number and the vehicle’s owner may be readily*⁴³ *made*.” *Id.*

Whether or not FCPD has been proven to have already *misused* the capabilities of its ALPR technology such that personal vehicular travel information has been compromised, it is undeniable that those capabilities create a material *potential* for such misuse.⁴⁴ Defendants have formally stipulated that their ALPR program would be materially inadequate to satisfy the strictures of the Data Act. That *potential for misuse* is just the sort of *link* between the *total operations and components* of the ALPR system and the *networked* VCIN/DMV records that the Supreme Court entrusted this Court to look for.

³⁹ “Identifiable” means “able to be named or recognized”. *Identifiable*, Cambridge Dictionary, <https://dictionary.cambridge.org/us/dictionary/english/identifiable> (Jan. 29, 2019).

⁴⁰ It is notable that, in defining the scope of the ALPR system subject to remand, both the legislature and the Virginia Supreme Court used both terms, “*identifying* particulars” and “*identifiable* particulars”, *Neal* 295 Va. at 347 (quoting definitions in Va. Code § 2.2-3801 for “information system” and “data subject”, respectively) (emphasis added).

⁴¹ To “identify” means to “to establish the identity of”. *Identify*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/identify> (Jan. 29, 2019).

⁴² To “provide” something is “to supply or make [it] available”. *Provide*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/provide> (Jan. 29, 2019). A “means,” as used here, is defined as “something useful or helpful to a desired end.” *Means*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/means> (Jan. 29, 2019). To “discern” something means “to detect with senses other than vision”, “to recognize or identify as separate and distinct”, or “to come to know or recognize mentally”. *Discern*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/discern> (Jan. 29, 2019).

⁴³ “Readily” is ordinarily defined as “in a ready manner: such as: without hesitating”, or “without much difficulty: Easily”. *Readily*, Merriam-Webster.com, <https://www.merriam-webster.com/dictionary/readily> (Jan. 29, 2019).

⁴⁴ If Lt. Palenscar’s testimony about FCPD’s virtually unrestricted FOIA production practices are to be believed, see TR1 104:5-11, it seems quite likely that FCPD has already provided and will continue to provide—intentionally—John Doe’s ALPR records to Jane Roe or *vice versa*.

E. Had The Supreme Court Rejected The Idea That FCPD’s Link To DMV Might Be An Adequate “Means For Discerning” Vehicle Ownership, It Would Have Said So

Defendants asserted at trial that the Supreme Court had already considered and ruled, *sub silentio*, that the availability of DMV ownership information was insufficient to qualify as the “link” it was looking for between the ALPR license plate data and the identity of ADDCAR’s owner and likely driver. TR2 22:10-21. This reads far too much into a brief and unparticularized reference by the Supreme Court to the unparticularized proposition—which (as this Court noted during trial) is referenced almost daily in trials and hearings involving automobiles—that “the Police Department can readily access databases operated by the Virginia Department of Motor Vehicles (“DMV”) and can obtain ‘personal information’ from those databases using ALPR information, including social security numbers, dates of birth, and addresses.” *Neal* 295 Va. at 341. The Supreme Court was clearly not satisfied with this generalization in the absence of record evidence providing details on the scope of the ALPR record-keeping process and specific descriptions of the actual means, steps, and actions through which a tag number in the ALPR database could be linked to such DMV information. Consequently, despite a general acknowledgement of the availability of some type of access to the DMV database, the Supreme Court did not believe it could conclusively and accurately determine on appeal whether and to what extent such a “link” could be “readily made”:

In the present case, however, it remains to be seen whether a sufficient link can be drawn to qualify a license plate number as an “identifying particular.” Although the ALPR database does not contain any information related to the individual to whom a specific license plate number is registered, that does not mean that the total components of the Police Department’s ALPR record-keeping process do not provide a means for discerning that information. On the record before this Court, however, we cannot say whether or not such a means exists as part of the ALPR record-keeping process.


Neal 295 Va. at 348. If the Supreme Court had already rejected the idea that a link to such DMV information could satisfy the parameters of an “information system”, the remand would have been unnecessary. It also is unlikely the Supreme Court would have rejected the notion that the

VCIN/DMV network could be a sufficient “link” between an ALPR tag number and a vehicle owner without (a) knowing the actual nature, scope, methods, and manner in which such a connection is or can be made or (b) saying *anything* to that effect. Rather, the paucity of the record on such a link led the Supreme Court to direct the parties and this Court to determine whether the ALPR record-keeping process, considered as a whole, is broad enough to encompass such a link. Undisputed evidence, including Defendants’ own judicial admissions, establish that it is.

V. CONCLUSION

For any or all of the reasons set forth in this brief, and based upon the entire record (including prior proceedings and judicial admissions by the parties) in this matter, Plaintiff Harrison Neal prays that he be awarded judgment against the Defendants, along with such other and further relief as justice and the Data Act may require.


Respectfully Submitted,
HARRISON NEAL
By Counsel


Edward S. Rosenthal (VSB No. 15780)
Lana M. Manitta (VSB No. 42994)
Jennifer A. Lucey (VSB No. 83603)
RICH ROSENTHAL BRINCEFIELD MANITTA
DZUBIN & KROEGER, PLLC
500 Montgomery Street, Suite 600
Alexandria, Virginia 22314
(703) 299-3440 phone
(703) 299-3441 fax
Email: ESRosenthal@RRBMDK.com
Email: LManitta@RRBMDK.com
Email: JALucey@RRBMDK.com
Counsel for Harrison Neal, Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of February, 2019, I served a true and correct copy of the foregoing Brief by electronic mail and by first class mail, postage prepaid, to the following:

Kimberly P. Baucom, Esq.
Assistant County Attorney
12000 Government Center Parkway
Suite 549
Fairfax, Virginia 22035
Email: kimberly.baucom@fairfaxcounty.gov



Jennifer A. Lucey