IN THE

SUPREME COURT OF VIRGINIA

Record No. 191129

FAIRFAX COUNTY POLICE DEPARTMENT and,
COLONEL EDWIN C. ROESSLER, JR., CHIEF OF POLICE,
Appellants,

v.

HARRISON NEAL,
Appellee.

BRIEF *AMICUS CURIAE* OF THE RUTHERFORD INSTITUTE IN SUPPORT OF APPELLEE

John W. Whitehead (VSB 20361)
Douglas R. McKusick (VSB 72201)
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, Virginia 22911
(434) 978-3888
douglasm@rutherford.org

Counsel for Amicus Curiae
THE RUTHERFORD INSTITUTE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rudolph H. Heimanson, *Remedial Legislation*, 46 MARQ. L. REV. 216 (1962) 4

Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1 (2013) 17, 18

Steven D. Seybold, *Somebody's Watching Me: Civilian Oversight of Data-Collection Technologies*, 93 Tex. L. Rev. 1029 (2015) 22

Va. Advisory Legislative Council, Computer Privacy and Security, Va. S. Doc. No. 27 (1976) 5, 8, 9, 11, 19

You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements, American Civil Liberties Union (July 2013) (available at https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf) 17, 18

STATEMENT OF THE CASE

Amicus accepts the Statement of the Case as set forth in the Brief of Appellee Harrison Neal. *Amicus* also states that on May 1, 2020, *amicus* filed a motion pursuant to Va. Sup. Ct. R. 5:30(c) for leave to file this brief.

STATEMENT OF FACTS

Amicus accepts the statement of facts as set forth in the Brief of Appellee Harrison Neal.

STANDARD OF REVIEW

Amicus accepts the Standard of Review as set forth in the Brief of Appellee Harrison Neal.

ARGUMENT

I. The Purpose And Intent Of The Data Act Requires Affirmance Of The Finding And Judgment Below That FCPD's ALPR Data Is Stored In An "Information System"

The outcome of the instant lawsuit brought to compel Appellants Fairfax County Police Department and Department officials ("FCPD")

to stop collecting and storing information obtained using Automated License Plate Readers ("ALPRs") turns on the construction and application of Virginia's Government Data Collection and Dissemination Practices Act, Va. Code §§ 2.2-3800 et seq. ("Data Act"). In a previous appeal, this Court, after concluding that the pictures and data (such as the time, date, and location from which the image was captured) associated with license plate numbers is "personal information" covered by § 2.2-3801 of the Data Act, remanded the case for a determination of whether a covered "information system" is involved. Specifically, this Court remanded "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." *Neal v. Fairfax Cnty. Police Dept.*, 295 Va. 334, 348 (2018).

Amicus submits that on remand the Circuit Court correctly found that FCPD practices with respect ALPR data constitutes an "information system" for purposes of the Data Act. This conclusion is inescapable when the history and purpose of the Data Act are considered. The Data Act, like other similar laws from around the

nation and world adopting fair information practices, was meant to limit the authority of the government to amass detailed and voluminous databases that can be used as "dossiers" to track, analyze and monitor the activities of individuals. The systems the Data Act was meant to regulate and restrict are those interconnected databases that the government can use, through the use of sophisticated mass surveillance technologies such as ALPRs, use to monitor the movements and activities of persons. The Circuit Court's finding that FCPD can readily and nearly instantaneously associate a captured license plate image with an individual, is exactly the kind of privacy invasion the General Assembly intended to prevent and prohibit by enacting the Data Act.

A. The Data Act's "Information System" Provision Should Be Liberally Construed And Applied

This Court's task in this case is to determine whether the Circuit Court correctly found that FCPD's ALPR system fit within the definition of an "information system" covered by the Data Act. That term is defined 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." Data Act § 2.2-3801. Thus, the question on appeal is whether the facts as found by the Circuit Court fit within this definition as properly construed.

As in any case of statutory interpretation, the primary aim is to give effect to the legislative intent. *Commonwealth v. Zamani*, 256 Va. 391, 395, 507 S.E.2d 608 (1998). If the intent is not plainly evident from the unambiguous language of the statute, resort may be made to aids to construction. *City of Virginia Beach v. Bd. of Supervisors of Mecklenburg County*, 246 Va. 233, 236 (1993).

In determining whether FCPD's ALPR data collection and use practices constitute a Data Act "information system," it must be borne in mind that this Court acknowledged in its previous decision in this case that the Data Act is a remedial statute. *Neal*, 295 Va. at 343-44. "Remedial statutes" are variously defined as "designed to correct an existing law, redress an existing grievance, or introduce regulations conducive to the public good." Rudolph H. Heimanson, *Remedial Legislation*, 46 MARQ. L. REV. 216 (1962). A basic rule of statutory interpretation is that remedial legislation is to be construed and applied

liberally. *Crone v. Richmond Newspapers, Inc.*, 238 Va. 248, 254 (1989); *Ballagh v. Fauber Enterprises, Inc.*, 290 Va. 120, 125, 773 S.E.2d 336 (2015). "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.'" *Neal*, 295 Va. at 344 (quoting *University of Virginia v. Harris*, 239 Va. 119, 124 (1990)).

The Data Act's remedial purposes are demonstrated by its text and the report that accompanied its enactment. The report of the Virginia Advisory Legislative Council that prompted enactment of the Data Act[1] pointed out that the revolution in automated data processing has given the government the capacity to compile detailed data on individuals, giving rise to fears that this will cause a chilling effect upon a free society. Va. Advisory Legislative Council, Computer Privacy and Security, Va. S. Doc. No. 27 at 3 (1976) (hereinafter "Va. S. Doc. No. 27"). The Legislative Council recommended enactment of fair data practices to prevent the emergence of abuse of the power of modern data systems. *Id.* at 8.

[1] The Data Act was originally titled the Privacy Protection Act. *Hinderliter v. Humphries*, 224 Va.439, 442 (1982).

Additionally, the General Assembly's findings contained in the Data Act's statutory text warned that individuals are directly affected by the extensive collection and maintenance of personal information, that great harm can occur from data collection and maintenance practices, and that "[i]n order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals." Va. Code § 2.2-3800(B).

More to the point of the issue before the Court now, i.e., whether the challenged practices constitute an "information system", the General Assembly's findings demonstrate that a broad concept of that term is required to serve the Data Act's remedial purposes. Thus, "[a]n individual's privacy is directly affected by the extensive collection, maintenance, *use and dissemination* of personal information[.]" Data Act § 2.2-3800(B)(1) (emphasis added). And "[t]he increasing use of *computers and sophisticated information technology* has greatly magnified the harm that can occur from these practices[.]" *Id.* § 2.2-3800(B)(2).

The Data Act was clearly meant to regulate the data practices of the government for the public good and, as such, is remedial legislation. It is meant to prevent government abuse of its power to collect and retain data and thereby preserve personal privacy.

The Data Act further shows that it was meant to cover and regulate the kind of interconnected systems that FCPD avails itself of in operating its ALPR system. Thus, as pointed out previously, the definition of an "information system" includes "*the total components* of a record-keeping process" and includes the management and use of data "by means of *computer networks* and the *Internet*[.]" Data Act § 2.2-3801 (emphasis added). Contrary to the suggestion of FCPD, the General Assembly did not take an approach that limited the Data Act's coverage to each discrete sector of government data management; instead, it broadly defined an "information system" as "the total components of a record-keeping process." Furthermore, the Act's coverage was extended to include the situation, such as that presented by the instant case, where the management and use of data is through the use of "computer networks" or "the Internet." Plainly, the General Assembly recognized that the dangers posed by the aggregation and

collection of personal information were presented, and indeed are amplified, when that information is allowed to be interconnected and agencies are allowed to tap into the personal data held by other government entities.

This is also reflected in Va. S. Doc. No. 27, the report that was the basis for the Data Act. The Advisory Council warned of the expanding data keeping and data processing capabilities of the government and the threat it posed to personal privacy. Va. S. Doc. No. 27 at 7. Because of this danger, it recommended as follows:

> To prevent the emergence of cases of abuse to prevent the tremendous potential power of *intercommunicating, automated, computerized personal data systems*, the Council recommends the enactment of a code of "fair data practices", based on the approach employed by codes of "fair labor practices."

Id. at 8 (emphasis added). It went on to advise the General Assembly that

> it would be well-advised to avoid gross abuse of the power of *intercommunicating data banks* by setting reasonable, easily implemented standards of conduct. Well managed, responsible data systems are as essential to the orderly and efficient operation of modern business, industry and government as uncontrolled, unrestricted gathering of total information dossiers about total populations are antithetical to a free society.

Id. at 11 (emphasis added).

Thus, in enacting the Data Act, the General Assembly had been specifically warned about the dangers of "intercommunicating data banks" and the need to regulate those in the interest of freedom and personal privacy. The General Assembly not only adopted verbatim the language suggested by the Advisory Council for the definition of an "information system," *id.* at 14, but it expanded and broadened that definition by including language that such a system also encompasses "information collected or managed by means of computer networks and the Internet[.]" Data Act § 2.2-3801. Clearly, the remedial purposes of the Data Act include regulating the kind of connection between information and databases that was shown below to exist with respect to FCPD's operation of its ALPR system.

B. The Studies Prompting Enactment Of The Data Act Warned Of The Danger To Privacy Created By Linked And Interconnected Computer Systems And Databases

Construction and application of the Data Act also should reflect the concerns that drove the movement to limit government collection and use of personal information of which it was a part. The Data Act was originally enacted in 1976 at a time when governments and policy

makers around the world were seeking to address the threat posed by the collection of information about individuals. Particularly noteworthy is the 1973 report of the U.S. Department of Health, Education and Welfare (HEW) examining the dangers posed by the growing use of automated data systems containing vast amounts of information about individuals. *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems¸ U.S. Dept. of Health, Education and Welfare (July 1973) (available at https://www.justice.gov/opcl/docs/rec-com-rights.pdf) (hereafter "HEW report"). The HEW report recommended the establishment of "fair information practices" ("FIP") by the government and private sectors, embodying the following principles:

> - There must be no personal-data record-keeping systems whose very existence is secret;
> - There must be a way for an individual to find out what information about him is in record and how it is used.
> - There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
> - There must be a way for an individual to correct or amend a record of identifiable information about himself.
> - Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their

> intended use and must take reasonable precautions to prevent misuse of the data.

Robert Gellman, *Fair Information Practices: A Basic History*, at 4-5 (2019), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

These FIP principles from the HEW report became the foundation for the Data Act, in which the General Assembly specifically articulated as required "principles of information practice" several FIP principles. Va. Code § 2.2-3800 (C). Indeed, Va. S. Doc. No. 27 that preceded enactment of the Data Act notes that a Senate Joint Resolution calling for the study of computer privacy and security specifically refers to the 1973 HEW report and "calls for the creation of a code of fair information practices for all automated data systems[.]" Va. S. Doc. 27 at 4. A subsequent Joint Resolution similarly expressed that all personal information systems initiated and maintained by any public or private organization should be operated in conformity with "principles of fair information practices." *Id.* at 5.

The language and history of the Data Act demonstrate the General Assembly's reliance the HEW report and the FIP principles espoused in that report as a way to address the concerns about data

systems and collections identified in the HEW report. Thus, the Data Act should be construed and applied so as to address the concerns expressed in the HEW report.

A key fear expressed in the HEW report is that data collected by different entities (government and otherwise) would be shared through interconnected computer systems. It noted that one way of creating an intelligence record or dossier is through combining bits and pieces of personal data from various records:

> [P]ublic concern about such combinations of data through linkings and mergers of files is well founded since any compilation of records from other records can involve crossing functional as well as geographic and organizational boundaries.

HEW report at 20-21. The report also acknowledged the "public fear of a 'Big Brother' system, in effect a pervasive network of intelligence dossiers" maintained and accessed through a network of computers. HEW report at 29.

The report went on to make recommendations for personal data systems and safeguards for the administration of such systems. In doing so, the HEW report defined an "automated personal data system" as "a collection of records containing personal data that can be

associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files." HEW report at 49. Significantly, the report also states that "[a] 'data system' includes *all processing operations*, from initial collection of data through *all uses of the data*." *Id*. (emphasis added).

The HEW report acknowledged the danger that linked computer systems would lead to the creation of personal dossiers, and so recommended regulations that defined in broad terms what constitutes a "personal data system" by including "all processing operations" and "all uses of data" as a part of a "system."

Because the Data Act grew out of and was modeled upon the HEW report, the term "information system" should be given the same broad scope. Doing so would clearly make FCPD's ALPR system an "information system." The ALPR system is readily and easily linked to other databases that serve to connect a license plate number to an individual.

II. The Data Act Is Meant To Restrict Government Surveillance Practices Such As Those Carried Out By ALPR Systems

The ruling below should be affirmed not only because it correctly applied the term "information system" of the Data Act, but also because it's extension of the Data Act to and ALPR system is consistent with the broader purposes of the Data Act and the kind of government information collection it was meant to prohibit. ALPRs collect a massive amount of data about the location and movement of vehicles, which can in turn be quickly and easily connected to individuals. It was precisely the aim of the Data Act to prevent the government from amassing dossiers on individuals that could be used to lay bare the details of their lives. The threat to privacy posed by ALPRs is exactly what the Data Act targeted, and this Court should enforce the Act by upholding the Circuit Court's decision.

A. ALPR Technology Is Part Of The Growing System Of Mass Surveillance And Collection Of Personal Information That Threatens Privacy

ALPR technology has the capability to capture the license number of passing cars at the rate of an astounding 1,800 per minute.[2] They have become a standard and commonplace tool of law enforcement throughout Virginia and the rest of the country. According to a 2013 Department of Justice survey, over three-quarters of police departments serving populations of over 100,000 residents utilized ALPRs,[3] and the number has no doubt grown since that time. Indeed, *amici* Commonwealth Attorneys who support FCPD and represent jurisdictions in every corner of the Commonwealth, assert that ALPR systems are used by many police departments throughout Virginia. Brief of *Amici Curiae* Twenty-Two Present and Former Commonwealth Attorneys, at 1-2.

In considering the scope of the information collected by ALPRs, it is well to note that, contrary to the implications contained in the briefs of FCPD and its supporting *amici*, collection is not limited to cameras mounted on police vehicles. ALPR cameras are located also in

---

[2] David J. Roberts and Meghann Casanova, "Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide," *International Association of Police Chiefs* (Aug. 2012), p. 2.
[3] Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia*, 25 RICH. J.L.& TECH. no.3, at 5 (2019).

stationary places, such as traffic lights and street poles, capturing and recording the license number of every vehicle that passes within the view of the camera.[4] These stationary ALPR cameras require no action or intervention by a police officer and allow the government to conduct surveillance of the activities of vehicles on highways 24 hours a day each and every day.

As a result, law enforcement agencies collect a huge trove of information on the activities of the individuals associated with those cars. As this Court wrote in the previous appeal, "[t]he images of the vehicle, its license plate, and the vehicle's immediate surroundings, along with the GPS location, time, and date when the image was captured 'afford a basis for inferring personal characteristics, such as . . . things done by or to' the individual who owns the vehicle, as well as a basis for inferring the presence of the individual who owns the vehicle in a certain location at a certain time." *Neal*, 295 Va. at 346-47. More recently, the U.S. Supreme Court recognized that it is a reasonable assumption that the registered owner of a vehicle is driving it at any particular time, *Kansas v. Glover*, No. 18-556, slip op. at 6 (U.S. Sup.

[4] Brooks, *supra*, at 1.

Ct. Apr. 6, 2020), meaning that the government can infer the activities of individuals based on data relating to vehicles.

Not only are FCPD and other law enforcement agencies collecting a vast amount of data, but "the overwhelming majority of people whose movements are monitored and recorded by these machines are innocent, and there is no good reason for the police to be keeping records on their movements. Ordinary people going about their daily lives have every right to expect their movements will not be logged into massive government databases." *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, American Civil Liberties Union (July 2013) at 13 (available at https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf).

Compounding matters is the fact that data collected by one agency can be shared or pooled with data collected by others. In addition to ALPR date and location data, governments have at their disposal other methods for identifying persons in public, such as surveillance cameras that employ biometric facial recognition technology.[5] This information

[5] Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 6 (2013).

can be combined to allow the government to essentially track persons as they go about their lives:

> Police can easily link a car's license plate number to a specific owner. And police can often use biometric information from surveillance cameras—commonly facial recognition—to identify a pedestrian on the street. Thus, once digitally efficient surveillance technologies collect data, this data can be linked or connected with a specific person through cross-reference to other government databases.[6]

With the cost of data storage decreasing, there is little reason or incentive for the government to purge this data, allowing it to amass data on individuals that was once unimaginable.[7] "Together these databases contain hundreds of millions of datapoints revealing the travel histories of [persons] who have committed no crime." *You Are Being Tracked*, *supra*, at 7.

Virginia's Data Act was enacted in order to prevent exactly this kind of stockpiling of information about persons. As pointed out above, the purpose of the Data Act was to "obviate the possibility of the emergence of cradle-to-grave, detailed dossiers on individuals, the existence of which dossiers would, 'at the push of a button,' lay bare to anyone's scrutiny, every detail, however intimate, of an individual's

---

[6] Rushin, *supra*, at 8.
[7] Rushin, *supra*, at 10.

life." Va. S. Doc. No. 27 at 7. Unrestrained use of ALPRs and collection of personal information by law enforcement is wholly inconsistent with the remedial purpose of the Data Act.

B. ALPR Data Collection, Storage And Use Is A Threat To Constitutionally-Protected Privacy Interests

Although the protections of the Data Act are not defined by, but are broader than, those provided by the federal and state constitutions, it is significant that collection and maintenance of ALPR data does threaten personal privacy interests within the protection of the Fourth Amendment. In *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court addressed whether long-term tracking of a vehicle using a global positioning satellite (GPS) device surreptitiously attached to the vehicle violated the owner's Fourth Amendment rights. Although the Court ruled that the trespassory attachment of the device to the vehicle violated the Fourth Amendment, four justices also opined in concurring opinions that long-term tracking of vehicles using advanced technology was also a constitutional violation:

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement

> agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving.

Jones, 132 S. Ct. at 964 (Alito, J., concurring).

More recently, the U.S. Supreme Court recognized the danger to privacy posed by the collection of cell-site location information (CSLI) and its use to track individuals. In *United States v. Carpenter*, 138 S. Ct. 2206 (2018), the Court rejected the government's claim that persons have no expectation of privacy in the records of their cell phone carriers showing the location of a person's cellphone. "Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Carpenter*, 138 S. Ct. at 2217. It warned against allowing the government unrestricted access to such data because it could be used to monitor the movements of persons:

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's

> movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.

Id. at 2218.

The collection of ALPR data at issue in this case poses precisely the same danger to privacy interests. Through analysis of the data obtained with ALPRs, which can be combined with other data obtained by surveillance technologies, law enforcement is able to determine the movements of a vehicles over long periods of time. Indeed, FCPD's current policy is to retain ALPR data for 365 days, allowing it to monitor and catalog the movements of persons for an entire year. As the Circuit Court found below, this information is easily linked to the driver and, along with other information collected by the government, can establish precisely the kind of "dossier" the Data Act was meant to forbid. "By analyzing all the information collected by data-collection technologies, police department can draw 'surprisingly powerful inference' from a collection of normal behaviors; the aggregated data

may reveal private ideas, beliefs, and values that are otherwise not discernable from a particular piece of information." Steven D. Seybold, *Somebody's Watching Me: Civilian Oversight of Data-Collection Technologies*, 93 Tex. L. Rev. 1029, 1039 (2015).

CONCLUSION

The Data Act was enacted at a time when the General Assembly was just beginning to appreciate the threat to individual liberty and personal privacy posed by emerging computer technology. The General Assembly could not have imagined the developments in information collection, storage, and analysis that have occurred in the last 40 years. Those developments, including ALPRs, have increased exponentially the dangers that led to the Data Act's enactment. If the purposes of the Data Act are to be fulfilled, it must be construed to include FCPD's ALPR data collection and its use as falling within the definition of an "information system." Therefore, the judgment of the Circuit Court below should be affirmed.

Respectfully submitted,

THE RUTHERFORD INSTITUTE

By /s/ Douglas R. McKusick
Counsel

John W. Whitehead (VSB 20361)
Douglas R. McKusick (VSB 72201)
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, Virginia 22911
(434) 978-3888
johnw@rutherford.org
douglasm@rutherford.org

Counsel for Amicus Curiae
THE RUTHERFORD INSTITUTE

CERTIFICATE OF COMPLIANCE AND SERVICE

The undersigned does hereby certify that the foregoing Brief *Amicus Curiae* of The Rutherford Institute in Support of Appellee complies with Va. Sup. Ct. R. 5:26. The undersigned further certifies that on May 15, 2020, a copy of the foregoing Brief *Amicus Curiae* of The Rutherford Institute in Support of Appellee was served upon all counsel in the case by emailing a true and correct electronic copy to each of the following:

Edward S. Rosenthal
RICH ROSENTHAL MANITTA & KROEGER, PLLC
500 Montgomery Street, Suite 600
Alexandria, Virginia 22314-2229
erosenthal@rrbmdk.com

Stuart A. Raphael
HUNTON ANDREWS KURTH LLP
Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, Virginia 23219
sraphael@HuntonAK.com

Elizabeth D. Teare
Office of the County Attorney
1200 Government Center Parkway, Suite 549
Fairfax, Virginia 22030
elizabeth.teare@fairfaxcounty.gov

/s/ Douglas R. McKusick