SCV: Submitted on 08-01-2017 14:58:33 EDT for filing on 08-01-2017

IN THE

Supreme Court of Virginia

RECORD NO. 170247

HARRISON NEAL,

Appellant,

v.

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

Appellees.

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

John W. Whitehead (VSB 20361)
Douglas R. McKusick (VSB 72201)
THE RUTHERFORD INSTITUTE
Post Office Box 7482
Charlottesville, Virginia 22906
(434) 978-3888
(434) 978-1789 (fax)
douglasm@rutherford.org

Counsel for Amicus Curiae

LANTAGNE LEGAL PRINTING 801 East Main Street Suite 100 Richmond, Virginia 23219 (804) 644-0477
A Division of Lantagne Duplicating Services

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

STATEMENT OF THE CASE 1

ASSIGNMENTS OF ERROR 1

STANDARD OF REVIEW 1

ARGUMENT 1

I. The Purpose and Intent of the Data Act Requires Including ALPR Data As "Personal Information" 1

A. The Data Act's "Personal Information" Provision Should Be Liberally Construed 3

B. The Data Act Is an Example of Fair Information Practices (FIP) Legislation and Adopted Prevailing and Ordinary FIP Principles 6

C. The Data Act Should Be Construed to Have a Scope Similar to Other FIP Legislation and Regulations and Cover ALPR Data Collection 9

1. "Personal Information" is defined broadly compared to other FIP laws and regulations 11

2. Other FIP laws and regulations cover information that is "identifiable" to an individual 13

3. The construction given "personal information" by the lower court does not reflect the legislative intent of the Data Act. 16

II. The Data Act Is Meant to Restrict Government Surveillance Practices Even If the Practices Do Not Violate the Fourth Amendment 20

CONCLUSION 23

CERTIFICATE OF SERVICE 25

TABLE OF AUTHORITIES

Cases

Ballagh v. Fauber Enterprises, Inc., 290 Va. 120, 773 S.E.2d 336 (2015).....4

Commonwealth ex rel. Dept. of Corrections v. Brown, 259 Va. 697, 529 S.E.2d 596 (2000).....4

Commonwealth v. Zamani, 256 Va. 391, 507 S.E.2d 608 (1998).....3

Crone v. Richmond Newspapers, Inc., 238 Va. 248, 384 S.E.2d 77 (1989).....4

Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982).....5

Katz v. United States, 389 U.S. 347 (1967).....20

Mapp v. Ohio, 367 U.S. 643 (1961).....21

United States v. Jones, 132 S. Ct. 945 (2012).....22

Statutes

18 U.S.C. § 2710(a)(3).....11

42 U.S.C. § 1983.....21

5 U.S.C. § 552a.....7

Va. Code § 2.2-3800..... passim

Va. Code § 2.2-3801.....3, 4, 12, 18

Other Authorities

Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* (2016).....10

Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877 (2014).....16

Paul M. Schwartz & David J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 84 N.Y.U. L.Q. Rev. 1814 (2011).....11, 13, 14, 19

Robert Gellman, *Fair Information Practices: A Basic History* (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020 .....7, 14, 15, 16

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) 13

Steven D. Seybold, *Somebody's Watching Me: Civilian Oversight of Data-Collection Technologies*, 93 Tex. L. Rev. 1029 (2015) 23

Va. Advisory Legislative Council, Computer Privacy and Security, Va. S. Doc. No. 27 (1976) 5, 8, 9, 17, 19

Rules

Va. Sup. Ct. R. 5:30(c) 1

Treatises

2B Sutherland Statutory Construction § 52:3 (7th ed.) 10

Constitutional Provisions

U.S. Const. Amend. IV ..... passim

STATEMENT OF THE CASE

Amicus accepts the Statement of the Case as set forth in the Opening Brief of Appellant Harrison Neal. *Amicus* also states that on July 14, 2017, *amicus* filed a motion for leave to submit this brief pursuant to Va. Sup. Ct. R. 5:30(c).

ASSIGNMENTS OF ERROR

Amicus accepts the Assignments of Error as set forth in the Opening Brief of Appellant Harrison Neal.

STANDARD OF REVIEW

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

ARGUMENT

I. The Purpose and Intent of the Data Act Requires Including ALPR Data As "Personal Information"

The outcome of the instant lawsuit brought to compel Appellees 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"). Specifically, this case involves the proper scope and construction of the term "personal information" contained in § 2.2-3801 of the Data Act. In denying Appellant Harrison Neal's request that FCPD be ordered to cease collecting and storing ALPR data unconnected with an active law enforcement investigation, the Circuit Court decided that the license plate numbers collected and stored by ALPRs are not personal information because (1) the numbers do not relate or connect directly to an individual, Letter Op. at 5, and (2) the numbers are publicly disclosed, so there is no expectation of privacy under the Fourth Amendment. Letter Op. at 6.

Amicus submits that the Circuit Court erred and that ALPR data consisting of the capture of license plate numbers along with the date, time and place of the capture is "personal information" 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" of the activities of individuals. The Circuit Court's crabbed reading of the scope of "personal information"

fails to appreciate that the ALPR data collected by FCPD does reveal something "about an individual," Va. Code § 2.2-3801, when considered with other information collected by the Commonwealth and so is covered by the Data Act.

Additionally, the Circuit Court's reliance on expectations of privacy under U.S. Const. Amend. IV as defining the scope of "personal information" is contrary to the purpose of the Data Act, which is to limit the collection of even information that is not "private" in the constitutional sense. The Data Act is meant to impose limits on government collection of information in addition to any limits that the constitution imposes because the General Assembly recognized the danger to privacy and security posed by the massive collection of information about persons.

A. The Data Act's "Personal Information" Provision Should Be Liberally Construed

This Court's task in this case is to determine the scope and application of the term "personal information" in the Data Act. 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.

Commonwealth ex rel. Dept. of Corrections v. Brown, 259 Va. 697, 529 S.E.2d 596 (2000).

In this case, "personal information" is broken into two categories: (i) information that "describes, locates or indexes anything about an individual", and (ii) information that "affords a basis for inferring personal characteristics." Va. Code § 2.2-3801. While the Data Act contains several examples under both of these categories, the statute makes clear that these examples are not exclusive and that they are meant merely to be descriptive of the kind of information within the scope of the Data Act. Ultimately, the language of the statute does not explicitly provide that ALPR collected data is "personal information."

In determining whether ALPR data is covered by the Data Act, it should be borne in mind that the Data Act is a remedial statute. "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, 384 S.E.2d 77 (1989); *Ballagh v. Fauber Enterprises, Inc.*, 290 Va. 120, 125, 773 S.E.2d 336 (2015).

The Data Act is remedial legislation as demonstrated by its text and the report that accompanied its enactment. The General Assembly found 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). Additionally, 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.

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

[1] The Data Act was originally titled the Privacy Protection Act. *Hinderliter v. Humphries*, 224 Va. 439, 442, 297 S.E.2d 684 (1982).

and thereby preserve personal privacy. The concept of "personal information" is crucial to achieving that legislative purpose because the construction and scope given "personal information" determines the protection that will be provided to citizens by the Data Act. Thus, "personal information" should be construed and applied liberally to achieve the remedial purpose of the Data Act.

B. The Data Act Is an Example of Fair Information Practices (FIP) Legislation and Adopted Prevailing and Ordinary FIP Principles

The statutory provisions which now make up the Data Act were 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. In 1973, the U.S. Department of Health, Education and Welfare (HEW) issued a report in response to the growing use of automated data systems containing vast amounts of information about individuals. The 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 2-3 (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

These FIP principles became the foundation for legislative action in the United States and elsewhere regulating government collection of information about individuals. The Privacy Act of 1974 reflects these principles. *See* 5 U.S.C. § 552a(e) (requiring federal agencies to, *inter alia*, only maintain information on individuals relevant to its purpose). Several European countries also adopted privacy laws embodying FIP principles, culminating in the Council of Europe's adoption in 1980 of a "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Gellman, *supra*, at 6. That same year, the Organization for Economic Cooperation and Development (OECD) adopted guidelines implementing FIP principles, including "[t]he purposes for which personal data are collected should be specified not later than at the time of the data

collection and the subsequent use limited to the fulfillment of those purposes[.]" *Id.* at 7.

The Data Act is another example of legislation embracing the FIP principles and is clearly within the mainstream of legislation seeking to protect citizens from the collection and maintenance of personal data. The General Assembly specifically articulated as required "principles of information practice" several FIP principles, including:

> 1. There shall be no personal information system whose existence is secret.
>
> * * * * *
>
> 6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.
>
> 7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.
>
> * * * * *
>
> 9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.

Va. Code § 2.2-3800(C).

That the statutory language echoes FIP principles is not surprising given the references to those principles in the Legislative Council's report that preceded enactment of the Data Act. Thus, the report notes that a Senate Joint Resolution calling for the study of computer privacy and security refers to the 1973 HEW 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 that the General Assembly intended it to further ordinary FIP principles and not to stake out an unusual or different position on data collection and use. The Data Act adopted what were and are consensus principles of information privacy law.

C. The Data Act Should Be Construed to Have a Scope Similar to Other FIP Legislation and Regulations and Cover ALPR Data Collection

The fact that the General Assembly embraced FIP principles that are embodied in other laws and regulations governing information collection and privacy is significant in construing the scope and effect to be given the Data Act in general and the term "personal information" in particular. If the Data Act was meant to reflect prevailing views on protecting information privacy, then it should be construed and applied in a manner that is consistent with the scope of other privacy laws and regulations.

This is consistent with statutory construction rules which look to the laws of other jurisdictions on similar subjects. "Legislation in other states and jurisdictions may help guide the interpretation of a doubtful statute which pertains to the same subject matter, person, things or relations. . . . Courts look to the phraseology and language of similar legislation not only in the interests of uniformity, but also to determine the general policy and objectives of a particular course of legislation. Foreign decisions involving similar factual situations have also been helpful to interpret doubtful statutes." 2B Sutherland Statutory Construction § 52:3 (7th ed.).

Thus, the construction to be given "personal information" as used in the Data Act should be consistent with the construction given similar terms in other information privacy laws. Given the General Assembly's embrace of FIP principles in the Data Act, there is every reason to give the Act's provisions, including "personal information", a scope consistent with that given in other laws. As noted in one work on privacy law:

> The concept of [FIPs] has powerfully influenced the development of modern privacy law. Simply stated, Fair Information Practices set out the rights and responsibilities for the collection of personal data. . . There are many conceptions of FIPs, but they all share a common architecture, assigning rights and responsibilities to data subjects and data holders.

Anita L. Allen & Marc Rotenberg, *Privacy Law and Society*, at 755 (2016).

1. "Personal Information" is defined broadly compared to other FIP laws and regulations. In this vein, it is important to point out that the Data Act's definition of "personal information" has unusual features that warrant reading that term at least as broadly as other similar terms used in information privacy laws. Information privacy laws use three different approaches to defining the scope of protected personal information:

- Tautological Approach: this approach uses a standard to define what information is protected. For example, the Video Privacy Protection Act protects against disclosure of "personally identifiable information," which is defined as "information which identifies a person[.]" 18 U.S.C. § 2710(a)(3). "The virtue of the tautological approach, like that of other kinds of standards, is that it is open rather than closed in nature. As a standard, it can evolve and remain flexible in response to new developments." Paul M. Schwartz & David J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 84 N.Y.U. L.Q. Rev. 1814, 1829 (2011).
- Non-Public Approach: this defines protected information "by focusing on what it is *not*, rather than on what it is. . . . Instead of saying [protected information] is simply that which identifies a person, the non-public approach draws on concepts of information that is

publically accessible and information that is purely statistical" and excludes these from protection. *Id.* at 1830.

- Specific-Types Approach: this approach lists specific types of data that constitutes protected information. The list operates as a rule, as opposed to a standard, and operates to include specified information within the scope of the law's protection if it falls within an enumerated category. *Id.* at 1831.

The Data Act's definition of "personal information" is a hybrid embracing both the tautological and specific-types approaches. "Personal information" is defined according to standards and includes all information that "(i) describes, locates or indexes anything about an individual" or "(ii) affords a basis for inferring personal characteristics[.]" Va. Code § 2.2-3801. Under each standard, the Data Act lists specific information that is deemed "personal information", such as social security numbers, voice prints or a record of the person's presence. Significantly, the specific-types list under each standard is expressly *not* exclusive—the General Assembly directed that "personal information" is "not limited to" the listed items or that protected information includes information "such as" the listed items.

By using both a tautological and non-exclusive specific-types approach to define "personal information" the General Assembly plainly

sought to adopt a broad and comprehensive approach to information protected by the Data Act. This hybrid approach is unique in its breadth and is unlike other approaches to defining protected information described in scholarly writings on the subject. Paul M. Schwartz & David J. Solove, *supra*, 84 N.Y.U. L.Q. Rev. at 1828-32. *See also* Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 Brook. L. Rev. 1, 46 (2013) (including Virginia among states that "have passed relatively broad laws that regulate the retention of data by government in all forms."). Moreover, that "personal information" is to be given a broad application is indicated by the fact that the Data Act sets forth two standards—it includes all information that (i) describes, locates or indexes anything about an individual or (ii) affords a basis for inferring personal characteristics. Va. Code § 2.2-3800. Clearly, the General Assembly intended "personal information" to have a wide coverage.

2. <u>Other FIP laws and regulations cover information that is "identifiable" to an individual</u>. Because the Data Act was modeled on FIP principles, what constitutes "personal information" under the Data Act also should have a similar scope to information protected under other FIP laws and regulations. FIP laws and regulations almost universally cover the collection and use of more than just information that directly identifies an

individual, which is the scope of coverage given by the Circuit Court below to "personal information" as used in the Data Act. Instead, mainstream FIP regulations cover information that *can be used* to identify a person or individual.

The central concept in information privacy law is to restrict collection and use of "personally identifiable information" ("PII"). The concept arose because of the increasing use of computers and their ability to connect information to people. Computerized records allowed analysis of many more pieces of personal data and linked the data to individuals:

> This development obliged policy makers to explore a novel set of issues regarding the kinds of information and the nature of the linkages that should trigger the application of information privacy laws. . . . No longer was it possible to assume privacy could be protected solely by safeguarding information involving a person's name or likeness. The scope of information requiring privacy protection became significantly larger—and also less clear and contestable.

Paul M. Schwartz & David J. Solove, *supra*, 84 N.Y.U. L.Q. Rev. at 1821. The 1973 HEW privacy report, cited by the 1976 Computer Privacy and Security report, Va. Sen Doc. No. 27 at 4, also referred to information held "in individually identifiable form[.]" Gellman, supra, at 42.

Thus, information privacy laws adopted under the FIP model extend protection to personally *identifiable* information, not only information directly identified with an individual. For example, the U.S. Department of

Homeland Security has promulgated Fair Information Practice Principles which restrict the collection, use, dissemination and maintenance of "personally identifiable information." Gellman, *supra*, at 21. Similarly, a White House report by the National Strategy for Trusted Identities in Cyberspace (NSTIC)[2] provides guidelines for the collection, use, dissemination and maintenance of "personally identifiable information." Gellman, *supra*, at 23.

Other statements of FIP principles state more clearly that the scope of information that is protected encompasses information that can be connected to a specific individual. The Department of Commerce has issued a report that included a Bill of Rights for protecting consumer privacy in the global digital economy that includes FIP principles. It provides that the Bill of Rights "applies to personal data, which means any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific

[2] The NSTIC "seeks to better protect consumers from fraud and identity theft, enhance individuals' privacy, and foster economic growth by enabling industry both to move more services online and to create innovative new services. The NSTIC aims to make online transactions more trustworthy, thereby giving businesses and consumers more confidence in conducting business online." White House, Office of the Press Secretary, "Administration Releases Strategy to Protect Online Consumers and Support Innovation and Fact Sheet on National Strategy for Trusted Identities in Cyberspace," April 15, 2011,https://obamawhitehouse.archives .gov/the-press-office/2011/04/15/administration-releases-strategy-protect-online-consumers-and-support-in.

computer or device." Gellman, *supra*, at 25. A Federal Trade Commission report on privacy that set forth a framework specifically intended to be consistent with FIP principles states that the framework "applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer or other device[.]" Gellman, *supra*, at 28. The European Union adopted a data protection directive that protects "personal data," defined as "information relating to an identified or identifiable natural person." An "identifiable" person was in turn defined as "one who can be identified, directly or indirectly[.]" Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877, 882 (2014).

These examples illustrate a consensus that the coverage of FIP laws and regulations extends beyond data directly identifying individuals and encompasses data and information that can be linked to and thereby indirectly identify individuals. As pointed out in one article on the subject: "In our view, identified information is present when a person's identity has been ascertained, or when there is a substantial risk of identification of a specific person by a party likely to obtain that information." Schwartz & Solove, *supra*, 102 Cal. L. Rev. at 877.

3. <u>The construction given "personal information" by the lower court does not reflect the legislative intent of the Data Act</u>. The Circuit Court's

construction of "personal information" under the Data Act is entirely too limited and conflicts with the scope of FIP laws and regulations the Act was meant to mirror. It determined that ALPR data is directly linked to a motor vehicle, not a person, and so that data is not "personal information." Letter Op. at 5.

But as pointed out above, ordinary FIP principles and the laws and regulations furthering those principles do not require that collected information *directly* identify an individual, and there is every reason to construe the Data Act's term "personal information" consistent with other FIP laws and regulations. First, as discussed above, it is clear that the General Assembly intended to bring the Data Act within the ordinary principles of information privacy law as espoused by FIP regulations. This is demonstrated by the statement of findings and principles set forth in Va. Code § 2.2-3800, which reference FIP principles and mandate that the Commonwealth and its political subdivisions adhere to those principles. These principles were similarly set forth in the Computer Privacy and Security Report that was the basis for the enactment of the Data Act. Va. S. Doc. No. 27, at 8-9. The Data Act was meant to advance standard FIP principles, which would include covering as "personal information" data that indirectly identifies an individual.

Moreover, the fact that "personal information" includes all information that "affords a basis for *inferring* personal characteristics", Va. Code § 2.2-3801, is further indication that the Data Act applies to information that can be linked to an individual. Almost by definition, identification by inference involves something other than direct identification. If, as the Circuit Court determined, it is required that data must directly identify an individual to qualify as "personal information," the "inferring" provision would be largely superfluous. By including data that affords a basis for "inferring personal characteristics" within the scope of "personal information," the General Assembly obviously intended to reach more than just direct identification data.

Finally, the Data Act was meant as a response to the increasing power of computers to store and analyze information from different data bases, giving the government the ability to know intimate details of the lives of individuals. In the study that led to the Data Act, the Legislative Council wrote:

> The revolution in the use of automated data processing equipment—particularly the electronic computer—has given government and private industry the capacity to compile detailed data on individuals in almost all areas of personal security. . . . Fears have been expresses as to the possibly chilling effect the existence of such collection of automated personal data systems can have upon a free society.

Va. S. Doc. No. 27 at 3. It urged the General Assembly 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 life." *Id.* at 7.The Council went on to recommend enactment of a "fair data practices code" in order "[t]o prevent the emergence of cases of abuse of the tremendous potential power of inter-communicating, automated, computerized, personal data systems[.]" *Id.* at 8.

Thus, the evil the Data Act targeted was the collection of disparate pieces of information that could be linked and connected using computers in order to indirectly and through inferences determine intimate details of the lives of individuals. The Data Act sought to address the problem that it was no longer possible "to assume privacy could be protected solely by safeguarding information involving a person's name or likeness," and so collection of more than just directly-identifying data needed to be restricted. Paul M. Schwartz & David J. Solove, *supra*, 84 N.Y.U. L.Q. Rev. at 1821.

The Circuit Court's ruling here undermines that purpose by ruling that ALPR data is not "personal information" under the Data Act. Even if the data collected does not by itself identify a person, it is easily linked to other records showing that automobile captured in the data is owned and

registered to an identifiable individual. This in turn allows an inference to be drawn concerning that person, including that he was present at a place at a particular time.

In sum, the ruling below adopts an unduly restrictive construction of "personal information" that is contrary to the history of FIP legislation generally and the Data Act in particular, and fails to carry out the purpose of the General Assembly to restrict the government's ability to assemble dossiers on the activities of citizens. ALPR data is assuredly "personal information" under the Data Act, and *amicus* urges this Court to reverse the judgment below.

II. The Data Act Is Meant to Restrict Government Surveillance Practices Even If the Practices Do Not Violate the Fourth Amendment

The Circuit Court's reliance on Fourth Amendment privacy standards as a touchstone for the scope of "personal information" under the Data Act is also misplaced. It is true that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *Katz v. United States*, 389 U.S. 347, 351 (1967). But the Data Act was not meant to adopt Fourth Amendment standards in determining what is and is not "personal information." It would have made

little sense for the General Assembly to codify the protections of the Fourth Amendment because those protections are independently enforceable by citizens through the constitutionally-mandated suppression remedy in criminal cases, *Mapp v. Ohio*, 367 U.S. 643 (1961), or through an action for relief under federal civil rights laws, 42 U.S.C. § 1983.

Instead, as discussed at length *supra*, the Data Act was meant as a response to the government's legal acquisition, maintenance and use of information about individuals and the threat this poses to a free society. Thus, the FIP principles set forth in the Data Act do not forbid collection of data in a way that is illegal or invades an individual's expectation of privacy, but forbid collection of information "unless the need for it has been clearly established in advance." Va. Code § 2.2-3800(C)(2). And nothing in the definition of "personal information" indicates that its scope is in any way limited to information obtained in a manner that violates Fourth Amendment standards. Indeed, the Circuit Court's conclusion that there is no threat to privacy from the collection of information in which there is no Fourth Amendment expectation of privacy is directly contradiction by the General Assembly's finding that "[a]n individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information."

It is worth noting, nonetheless, that collection and maintenance of ALPR data does threaten interest that touch up Fourth Amendment interests. 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).

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, law enforcement is able to determine the movements of a vehicles over long periods of time. 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 ALPR data as “personal information." Therefore, the judgment of the Circuit Court below should be reversed.

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 22906
(434) 978-3888
Fax: (434) 978-1789
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 Respondent complies with Va. Sup. Ct. R. 5:26. The undersigned further certifies that on August 1, 2017, a copy of the foregoing Brief *Amicus Curiae* of The Rutherford Institute in Support of Appellant was served upon all counsel in the case by mailing, postage prepaid, three (3) true and correct copies thereof and one (1) true and correct electronic copy to each of the following:

Edward S. Rosenthal
RICH ROSENTHAL BRINCEFIELD MABUTTA
DZUBIN & KROEGER, LLP
201 North Union Street, Suite 230
Alexandria, Virginia 22314

Elizabeth D. Teare
Office of the County Attorney
1200 Government Center Parkway, Suite 549
Fairfax, Virginia 22030

/s/ Douglas R. McKusick
Douglas R. McKusick