AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY
Post Office Box 32159
Newark, New Jersey 07102
973-642-2086
ebarocas@aclu-nj.org http://www.aclu-nj.org

CONSTITUTIONAL RIGHTS CLINIC
Center for Law and Justice
123 Washington St.
Newark, NJ 07102
973 353-1127 TEL
973 353 1445 FAX
ronald.chen@law.rutgers.edu http://law. rutgers.edu

Comments to the Proposed Amendments to N.*J.A.C.* 13:21-8.2 and *N.J.A.C.* 13:82-8.20

November 30, 2015

Raymond P. Martinez, Chairman and Chief Administrator
c/o Kate Tasch, Administrative Practice Officer
Regulatory and Legislative Affairs
Motor Vehicle Commission
225 East State Street, PO Box 162
Trenton, NJ 08666-0162

Dear Chairman Martinez:

1. The American Civil Liberties Union of New Jersey and the Rutgers Constitutional Rights Clinic (the "Commenters") respectfully submits these comments regarding the proposed amendments to *N.J.A.C.* 13:21-8.2 and *N.J.A.C.* 13:82-8.20,[1] which were published October 5, 2015 (47 N.J. Reg. 2428).

2. The ACLU of New Jersey, the state affiliate of the national American Civil Liberties Union, is an organization with approximately tens of thousands of members and supporters statewide, dedicated to advancing the values enshrined in the Bill of Rights, as well as those protected in the New Jersey Constitution, including the right to privacy. The Rutgers Constitutional Rights Clinic, first established in 1970 as the Constitutional Litigation Clinic, engages in "impact" litigation and advocacy in the area of individual civil liberties and civil rights, including the right to privacy, as protected in the constitutions of the United States and the State of New Jersey.

3. In 2012, the ACLU-NJ initiated a lawsuit in the Superior Court of New Jersey, *ACLU-NJ v. Martinez*, in which it challenged implementation by the Commission of the "TRU ID" system as not consistent with the Administrative Procedures Act. After the court issued a temporary restraining order prohibiting implementation of TRU ID, the Commission and the ACLU-NJ reached a settlement agreement whereby the Commission agreed to retain the existing 6-point identification system without change, absent promulgation of proper regulations, written notice of which would be given to the ACLU-NJ. Commenter ACLU-NJ received written notice of these proposed regulations on October 8, 2015.

4. The proposed regulations would authorize the Commission to "to scan applications, declarations, and documents that are presented by the Commission's customers to satisfy the six-point identification system requirements when obtaining permits, licenses, and non-driver identification cards." The proposed amendments also indicate that the scanned applications, declarations, and documents will be retained electronically in accordance with Division of Revenue and Enterprise Services (DORES) statutes and retention schedules.

5. The notice states generally that the purpose of the proposed amendments "is to ensure the integrity of the Commission's six-point identification verification system by enabling the Commission to conveniently access and verify the application and documents that were submitted by the customer in order to obtain the Motor Vehicle Commission document." Neither the notice nor proposed regulations state explicitly that they are proposed in order to implement the proposed "TRU ID" system, or to bring New Jersey into compliance with the

[1] For ease of reference, each paragraph in these comments is numbered sequentially.

federal REAL ID Act, Pub. L. 109–13, 119 Stat. 302 (2005). Nevertheless, the effect of the proposed amendments would be to allow New Jersey to implement a key requirement of the REAL ID Act, which requires that the State retain copies of the "application, declaration and source documents" presented to obtain a REAL ID compliant identification. 6 C.F.R. § 37.31.

6. Enactment of these proposed amendments would effect a dramatic change in both the quality and quantity of private individual information that the Commission retains in a new digital data warehouse. As further explained below, Commenters believe that the proposed regulations do not adequately take into account the privacy interests of the people of New Jersey in at least two respects:

a. The Commission has not identified any substantial and legitimate need to *retain* copies of personal documents—which can contain extremely sensitive individual information—once the originals of those documents have already been inspected, and the identity of the applicant established, by an authorized MVC official.

b. Even if there were a legitimate need to retain copies of individual source documents, the proposed regulations (despite the cross-reference to the DORES statutes and retention schedules) do not provide for adequate safeguards to protect the security, confidentiality, and integrity of the personally identifiable information collected, stored, and maintained by MVC and that would guard against unauthorized disclosure. Nor does the reference to DORES retention schedules give adequate guidance on how long the documents will be retained.

I. The Commission Has Not Demonstrated that It Has any Need to Retain Individual Personal Documents that Would Outweigh the Intrusion into Privacy Interests.

7. The proposed scanning and retention of the millions of personal source documents presented each year to MVC by New Jersey residents vividly illustrates the now well-documented challenges to personal privacy brought about by "big data," i.e. advances in technology that allow both the storage and analysis of information—both digital and analog—on a scale previously impossible. As noted by the President's Council of Advisors on Science and Technology ("PCAST") in transmitting the *Report to the President, Big Data and Privacy: A Technological Perspective (*available at: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf):

> Big data drives big benefits, from innovative businesses to new ways to treat diseases. The challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible.
>
> Transmittal Letter to President Obama from John Holdren and Eric Lander, May 2014.

8. Commenters agree with the President's Council and others who have noted that any undertaking to collect and retain personal information on the scale proposed by the

Commission brings with it a concomitant obligation to adopt policy appropriately crafted to balance the State's need to collect and retain this information against unwarranted intrusions on personal privacy. Absent such an affirmative articulation of the *need* for such data retention, as well as a policy designed to prevent against unauthorized use and disclosure of such information, Commenters believe that the proposed regulations would be a per se arbitrary and unreasonable exercise of the Commission's rule-making authority.

9. Courts have also recognized a constitutional dimension to the intrusion on privacy caused by governmental collection and retention of personal information. "The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, *the degree of need for access*, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access." *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980) (emphasis added); *see also, C.N. v. Ridgewood Bd. of Educ.*, 430 F.3d 159, 179-80 (3d Cir. 2005).

10. The current list of source documents that might be potentially scanned and stored under the proposed amendments is exhaustive, and touches upon virtually all aspects of a private resident's life: health records, financial and asset records, educational records, familial status records, immigration records, tax records, and more. That list includes:

birth certificate

US passport

Current NJ digital driver license, boat license or non-driver ID card

Valid active duty US military photo ID card

US adoption papers

Certificate of naturalization

Certificate of citizenship

Civil marriage, domestic partnership or civil union

Order or decree of divorce, dissolution or termination

Court order for a legal name change, signed by a judge or court clerk

Current US military dependent card

US military photo retiree card

Valid NJ firearm purchaser card

US school photo ID card with transcript or school records

US college photo ID card with transcript

Valid federal, state or local government employee driver license

Valid federal, state or local government employee photo ID card

US military discharge papers

FAA pilot license

Current/expired less than one year non-digital NJ PHOTO driver license

Current photo driver license from any other U.S. state, the District of Columbia or the U.S. Territories of American Samoa and Guam, Puerto Rico or the U.S. Virgin Islands

Social Security card

Bank statement or record

ATM card with preprinted name and applicant's signature.

Current health insurance card, prescription card OR Employee ID card with printed pay stub

State professional license

NJ public assistance card with photo (also known as a NJ Social Services ID card)

High school diploma, GED or college diploma

Property tax statement, bill or receipt issued by a New Jersey municipality

For NJ high school students: a waiver certificate for the written portion of the driver's test

Veterans Affairs universal access photo ID card

Utility or credit card bill issued in the past 90 days

Checking or savings account statement from a bank or credit union, issued in the past 60 days

High school or college report card or transcript containing address, issued within the past two years

Original lease or rental agreement showing name as the lessee or renter

Property tax bill, statement or receipt from the past year

Any letter or correspondence (including tax bills) received from the IRS or state tax office in the last year

First-class mail received from any federal, state or local government agency in the past six months

Foreign passport with INS or USCIS verification and valid record of arrival/departure (Form I-94)

Foreign passport with INS or USCIS verification and valid Form I-551 stamp	US re-entry permit (Form I-327)	Current photo employment authorization card (Form I-688B or I-766).
Current alien registration card (new Form I-551) with expiration date and verification from INS or USCIS	Valid I-94 stamped "Refugee," "Parolee," "Asylee" or "Notice of Action" (Form I-797 approved petition) by INS or USCIS	Current alien registration card (old Form I-551) without expiration date and with INS or USCIS verification
Refugee travel document (Form I-571)	Valid I-94 with attached photo stamped "Processed for I-551…" by INS or USCIS	Photo temporary resident card (Form I-688)

11. Commenters acknowledge that the Commission has a legitimate interest in determining the correct identity and place of residence of any person seeking a New Jersey motor vehicle license or non-driver ID card. That interest has been quite satisfactorily addressed for many years through the current six point identification system, in which personal source documents are produced for *inspection* by a trained and authorized MVC official at the time of license issuance or renewal. The proposed amendments, however, trigger a requirement that the Commission demonstrate the need to *retain* scanned copies of those source documents in a new MVC data warehouse. The proposed amendments do not articulate, much less justify, the need to retain copies of the document, as distinct from the need to inspect them.

12. The notice states that the need for scanning and retention of source documents is "to ensure the integrity of the Commission's six point identification verification system by enabling the Commission to conveniently access and verify the application and documents that were submitted by the customer in order to obtain the Motor Vehicle Commission document." The notice in particular refers to the legislative findings contained in N.J.S.A. 39:2A-2, in which the Legislature noted that "Criminals have used counterfeit passports, Social Security cards, county identification cards, pay stubs and W-2 forms to obtain fraudulent driver's licenses and identification cards in furtherance of identity-theft schemes." N.J.S.A. 39:2A-2(i). The Legislature also cited the report of the Fix DMV Commission,[2] issued thirteen years ago in November 2002, to support the contention that "The DMV's failed security systems are contributing to a growing national problem of identity theft." The fraud referenced in the Fix DMV report was fraud perpetuated by former *DMV employees* in 2002.

13. Of course, the current six point identification system, cited nationally as a "best practice,"[3] was the major response to the problems identified by the Legislature in 2002, and by the Fix DMV Commission. The proposed amendments do not articulate in any detailed fashion how long term retention of source documents will significantly improve the Commission's ability to detect fraudulent activity *by the MVC customer*, as opposed to fraudulent activity by MVC employees. It is completely unclear why such future potential misconduct by MVC employees requires retention of mass quantities of personal information regarding MVC customers.

---

[2] http://www.state.nj.us/mvc/pdf/About/finalreport.pdf.

[3] New Jersey Motor Vehicle Commission, *4 Years of Progress, March 30, 2007 Service Assessment*, p.4, available at http://www.state.nj.us/mvc/pdf/About/March302007.pdf

14. If the Commission identified the proposed practice that would require regular reference to the source documents, then it might be possible to balance the need for such use against the intrusion into privacy. But absent such a systemic plan to discover customer fraud by reference to the retained source documents, retention of private records under a "just in case" rationale is the type of overreaching that, while made logistically possible by the advances in "big data," does not provide sufficient justification for widespread retention of private information without a particularized *use* of such information being identified.

II. The Commission's Failure to Provide for Safeguards Against Unauthorized Disclosure Renders Retention of Private Source Documents Unreasonable and Unlawful.

15. In addition to failing to articulate the need for retention of private source documents after having been inspected by the Commission, the proposed regulations fail to adequately describe the safeguards that it will implement to prevent this vast warehouse of private and identifiable information from unauthorized disclosure. Such safeguards are essential to protecting the individual's constitutional, statutory and common law privacy interests. *See Westinghouse*, 638 F.2d at 578; *compare Whalen v. Roe*, 429 U.S. 589, 605 (1977) (allowing collection of personal health information where statute imposed safeguards against unauthorized disclosure).

16. The proposed amendments make a sweeping incorporation by reference to "Division of Revenue and Enterprise Services (DORES) statutes and retention schedules." Inspection of the DORES statutes and retention schedules, however, reveal *no* procedures, practices of safeguards by which unauthorized disclosure would be prevented. And if the Commission is concerned about recent instances of misconduct by its own employees (see ¶12 above), then it must also take into account the recent instances in which MVC employees have been charged with selling confidential information.[4] The DORES statutes and retention schedules fails to define any standards that will sufficiently secure the sensitive information which is being retained by the DMV, or that will limit the government employees that have access to it.

17. Indeed, the proposed amendments do not even comply with federal requirements under the REAL ID Act. 6 C.F.R. § 37.31 requires that "States shall take measures to protect any personally identifiable information collected pursuant to the REAL ID Act as described in their security plan under § 37.41(b)(2)." 6 C.F.R. § 37.41(b)(2) in turn requires a state to adopt a security plan that contains, in part:

> Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act. These safeguards must include procedures to prevent unauthorized access, use, or dissemination of applicant

[4] *See* "Two Motor Vehicle Commission workers charged in identity theft," http://www.nj.com/mercer/index.ssf/2011/11/two_motor_vehicle_commission_w.html.

information and *images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction*.

(emphasis added).

18. The proposed amendments do not refer to any "administrative, technical, and physical safeguards" that prevent unauthorized access. The DORES statutes and retention schedules merely provide schedules for retention of classes of documents, not measures that protect against unauthorized access or disclosure. Moreover, the DORES retention schedules for state agencies currently do not even provide a destruction date for source documents retained by MVE (http://www.nj.gov/treasury/revenue/rms/pdf/G100000_007.pdf).[5] Nor do the proposed regulations comply with the particular privacy requirement of the REAL ID Act that, "Upon request by an applicant, a State shall record and retain the applicant's name, date of birth, certificate numbers, date filed, and issuing *agency in lieu of an image or copy of the applicant's birth certificate*, where such procedures are required by State law." 6 C.F.R. § 37.31(c) (emphasis added).

19. Indeed, the compilation of this vast amount of sensitive personal information will create a treasure trove for identification thieves, whether they are hackers or government employees. The database thereby seemingly creates more, rather than less, risk of fraud (especially where fraud by customers – as opposed to employees – has not been shown to be a significant issue absent the proposed retention of records).

20. Absent any adoption (through the appropriate rule-making process) of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the source documents retained by the Commission, adoption of these proposed amendments are an inherently unreasonable and arbitrary exercise of the Commission's rule-making authority.

III. Conclusion

21. The proposed amendments to N.*J.A.C.* 13:21-8.2 and *N.J.A.C.* 13:82-8.20 constitute a sea change in the amount of private information, and the nature of that information, that MVC will now retain concerning the motoring public in a data warehouse of unprecedented scope and size. Without further articulation of the *need* to retain such information, and a description of the security plan to guard against unauthorized disclosure, Commenters urge the Commission not to enact these amendments in their current form.

Respectfully submitted,

Edward Barocas
American Civil Liberties Union of New Jersey

Ronald K. Chen
Rutgers Constitutional Rights Clinic

[5] The REAL ID Act requires that such records be retained for 10 years. 6 C.F.R. § 37.31(a)(3).