



September 25, 2007

Clark J. Holloway  
Department of Licensing  
P.O. Box 9030  
Olympia, WA 98507-9030

Re: Proposed Rules for Washington's Enhanced Driver License and Identocard

Dear Mr. Holloway:

AMERICAN CIVIL  
LIBERTIES UNION OF  
WASHINGTON  
FOUNDATION  
705 2ND AVENUE, 3RD FL.  
SEATTLE, WA 98104  
T/206.624.2184  
WWW.ACLU-WA.ORG

JESSE WING  
BOARD PRESIDENT

KATHLEEN TAYLOR  
EXECUTIVE DIRECTOR

The ACLU of Washington (ACLU-WA) welcomes this opportunity to comment on the proposed regulations for the Enhanced Driver License program (EDL). The ACLU-WA is an organization of over 20,000 members in Washington dedicated to defending civil liberties, including privacy.

Based on our discussions with Department of Licensing staff, we believe that the department is dedicated to protecting the privacy of drivers who choose to participate in the EDL program. To provide clear guidance to both department staff and other states considering following Washington's efforts as a response to the Western Hemisphere Travel Initiative, the ACLU-WA urges you to incorporate the following recommendations for the draft EDL rules published as WSR 07-17-157.

1) Clearly describe the required privacy protections and safeguards.

The draft rules should explicitly spell out procedural safeguards and technical standards that the EDL program will rely on to protect privacy. ACLU-WA strongly supported the language in ESHB 1289 that directs the department to regularly update the rules to reflect technological innovations pertaining to the privacy and security of cardholders:

From time to time the department shall review technological innovations related to the security of identity cards and amend the rules related to enhanced driver's licenses and identicards as the director deems consistent with this section and appropriate to protect the privacy of Washington state residents.<sup>1</sup>

We urge the department to incorporate language into the rules that will provide a process for this regular review. Such language should clearly address internal procedures and limits regarding the access, use and disclosure of information acquired through the EDL program. Language should also establish the basis for technological innovation review, by specifically spelling out the intent to use the most privacy-protective technology and the standards that such technology must meet.

---

<sup>1</sup> Section 1 (3)(d)

2) Require that information about the use of RFID and facial recognition in the EDL be provided to the EDL applicant in writing before the application is processed.

Proposed WAC 308-105-020 sections (3) and (4) require card applicants to sign a declaration acknowledging the use of both facial recognition and RFID. As currently written, language does not require that the department staff give the applicant written information about facial recognition and RFID; it only says the applicant must be “given an opportunity to receive” information. Many applicants will be unfamiliar with the purpose, use and potential risks of these technologies.

We request that sections (3) and (4) be amended to explicitly require department staff to provide written information about the technologies prior to the applicant signing an acknowledgement.

3) The department’s notice to the applicant about RFID should be expanded to include the purpose, use and risks and should be incorporated within **WAC 308-105-020 (4)**.

While the ACLU-WA does not support the inclusion of RFID in the EDL, we applaud the department’s intent to inform individuals of RFID chip content and how the RFID component may be used. It is important that all of the components of the notice be given in plain English.

To avoid misuse or lax security, the department should fully inform individuals of the risks they assume when carrying an RFID tag that broadcasts a number unique to the cardholder. We understand the department is considering providing a sleeve for licenses. Applicants must first recognize the risks to privacy and understand the importance of such a shielding device before they would opt to use it. Applicants should also be notified of the limitations of such a shielding device.

The notice should also disclose: a) who will have system-based access to the department’s linkage between the RFID identifier number and the individual’s personal information, b) the risk of unauthorized reading of the RFID, c) the risk of independent association of RFID identifier and personal information by third parties and d) a list of all authorized locations where the EDL will be read by the department, border patrol or any other authorized entities. Such a list should be updated to reflect new reader locations as they are added.

We encourage the department to consider the attached language from California’s SB30 as a model for its notice.

4) The department should expand its notice to the applicant to include a description of how facial recognition is to be used, and should incorporate this within **WAC 308-105-020 (3)**.

The rule currently requires applicants to acknowledge that their photograph will be used as a facial recognition biometric identifier in a one-to-many matching system. We encourage the department specifically to note in the rules information about what dataset(s) individual photos will be matched against. It is currently unclear whether the matching will be against other EDL holders, standard license holders, or photos obtained outside of the department either by the federal government or third-party contractors.

Applicants should be provided with information explaining the facial recognition process, explicitly noting the source of the many photos against which an individual’s biometric will be compared. Such notice also should address potential errors in the biometric matching process and available recourse if an error occurs.

The rule also should spell out specific protections that will prevent parties outside of Washington's Department of Licensing from accessing a person's photo (i.e., biometric identifier). We are concerned that the photo will be later accessed through a national facial recognition system that does not carry the same protections as the system the department maintains in Washington. Such a practice of adding photos into a facial recognition dataset would violate the department's policy of using the biometric-identifier only for identity verification at the time of application.

5) Clarify language indicating that tampering and deactivation of RFID would invalidate its cross-border purpose.

Proposed language for WAC 308-105-020 (4) states that licenses and identicards with inactive RFID chips will be invalid for border crossing:

(4) An applicant for an enhanced driver's license or identicard must sign a declaration acknowledging that he or she has been notified that the enhanced driver's license or identicard contains a radio frequency identification chip, that he or she has been given an opportunity to receive information on the type of information the chip contains and how it may be used, **and that tampering with or deactivating the chip will invalidate the enhanced driver's license or identicard for purposes of border crossing.** (emphasis added).

Since a broken RFID tag will invalidate the license or identicard for border crossing, both the rule and the notice to the applicant should specify: a) the method(s) through which an individual will learn that their RFID tag is inactive and b) the process through which a cardholder can replace a license or identicard with an inactive RFID tag.

6) The department should provide applicants who are denied an EDL a specific explanation of the reason for the denial.

An applicant for a regular driver's license can fairly easily determine why he or she has been denied a license or identicard. An applicant for an EDL, however, may not be able to determine why the department denied the application. Given the added complexity of the systems behind EDL, it is increasingly important that individuals know the specific reason why they have been denied an enhanced license or identicard. An application could be denied for a perfectly valid reason or because the department is verifying the application data against erroneous information in another database. The department should ensure that data-matching and verification processes remain transparent, especially if an error exists in the government's system or if the government is relying on erroneous information in another system.

7) The language that permits third-party updates of the address of record should include a notice of the update to the EDL holder.

We understand that this language was added to accommodate a data system overseen by the U.S. Postal Service. It is important to confirm the address update with the individual to avoid erroneous changes, possibly resulting from identity theft. The department should notify the cardholder that it has updated their record, preferably by providing notice to both former and new addresses.

We welcome the opportunity to comment on these draft rules and are available to discuss our comments and future drafts in more detail.

Sincerely,

Christina Drummond  
Technology and Liberty Project Director  
American Civil Liberties Union of Washington Foundation