



**Testimony of Kimberly McCullough, Legislative Director
In Support of SB 641
House Committee on Judiciary
May 11, 2015**

Chair Barker and Members of the Committee:

For the record, my name is Kimberly McCullough, Legislative Director of the ACLU of Oregon. Thank you for the opportunity to submit comments in support of SB 641.

Data stored on a smartphone or other portable electronic device can paint a near-complete picture of even the most intimate and personal details of our lives. Before the age of smartphones, it was impossible for police to gather this much information about a person's communications, historical movements, and private life. Today, police officers routinely search the contents of a person's cell phone during an arrest or after a cell phone seizure. With increasing frequency, officers perform such searches with the aid of electronic devices that strip a cell phone of its data on the scene. This type of highly intrusive data mining implicates significant privacy concerns.

Tech companies are now marketing a wide variety of forensic devices and software to law enforcement that extract and duplicate the contents of portable electronic devices. Examples of these include MSAB's XRY Kiosk (a forensic tool designed to easily extract data in the field) and CelleBrite's UFED Touch (a standalone mobile forensic extraction device). These devices and software can:

- Crack passwords and user locks
- Decode encrypted data
- Recover deleted files
- Access remotely-stored data
- Access private online accounts, email, calendar and contact files
- Decode and compile location data to create detailed maps of where the portable electronic device has been

SB 641 contains the following provisions to protect Oregonians' privacy:

- Prohibits law enforcement from duplicating or copying data from a portable electronic device without a warrant or consent.
- Provides a remedy for violations: no information obtained without a warrant or consent can be used in a court or other proceeding, nor used to establish reasonable suspicion or probable cause that an offense has been committed. This remedy is available to the owner of the portable electronic device and other persons with a reasonable expectation of privacy in the contents of the device

- Authorizes court to order law enforcement to purge duplicated data if defendant files motion for return of property.

Please note that Oregon Department of Corrections and Oregon Youth Authority have reached out to us with concerns that this bill may impact their ability to forensically search electronic devices found in a correctional facility and devices belonging to individuals on parole or probation. We are working with DOC and OYA to craft language that will allow for forensic imaging of devices in circumstances when that is already allowed under current law without expanding DOC and OYA's authority.

Please also note that the Department of Justice raised concerns about the use of the word "appropriate" as a modifier of "consent" on page 1, line 20. We have agreed to change "appropriate" to "lawful," as we agree that "appropriate" would create a vague standard. The word "lawful," on the other hand, will give clear instruction to courts that consent should be voluntary and that the scope of consent given must include forensic imaging in order for such imaging to be performed by law enforcement.

We urge you to support SB 641. Please feel free to contact me with any questions or concerns.