(ii) electronic information or data transmitted by the owner of the electronic
information or data to a remote computing service provider.

(b) Except as provided in Subsection (1)(c), a law enforcement agency may not use, copy, or disclose, for any purpose, the location information, stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider, that is not the subject of the warrant that is collected as part of an effort to obtain the location information, stored data, or transmitted data of the electronic device that is the subject of the warrant in Subsection (1)(a):

(i) is not the subject of the warrant; and

(ii) is [incidentally] collected as part of an effort to obtain the location stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider that is the subject of the warrant in Subsection (1)(a).

(c) A law enforcement agency may use, copy, or disclose the transmitted data of an electronic device used to communicate with the electronic device that is the subject of the warrant if the law enforcement agency reasonably believes that the transmitted data is necessary to achieve the objective of the warrant.

(d) The electronic information or data described in Subsection (1)(b) shall be destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably possible after the electronic information or data is collected.

(2) (a) A law enforcement agency may obtain location information without a warrant for an electronic device:

(i) in accordance with Section 53-10-104.5;

(ii) if the device is reported stolen by the owner;

(iii) with the informed, affirmative consent of the owner or user of the electronic device;

(iv) in accordance with a judicially recognized exception to warrant requirements; [or]

(v) if the owner has voluntarily and publicly disclosed the location information; or

(vi) from the remote computing service provider if the remote computing service provider voluntarily discloses the location information:
use, copy, or disclose a subscriber record without a warrant:

(a) with the informed, affirmed consent of the subscriber or customer;
(b) in accordance with a judicially recognized exception to warrant requirements;
(c) if the subscriber or customer voluntarily discloses the subscriber record in a manner
that is publicly accessible; or
(d) if the provider of an electronic communication service or remote computing service
voluntarily discloses the subscriber record:
(i) under a belief that an emergency exists involving the imminent risk to an individual
of:
(A) death;
(B) serious physical injury;
(C) sexual abuse;
(D) live-streamed sexual exploitation;
(E) kidnapping; or
(F) human trafficking; or
(ii) that is inadvertently discovered by the provider, if the record appears to pertain to
the commission of:
(A) a felony; or
(B) a misdemeanor involving physical or sexual violence, or deception.
(5) A provider of an electronic communication service or remote computing service, or
the provider's officers, employees, agents, or other specified persons may not be held liable for
providing information, facilities, or assistance in good faith reliance on the terms of a warrant
issued under this section, or without a warrant in accordance with Subsection (3).
(6) Nothing in this chapter affects the rights of an employer under Subsection
34-48-202(1)(e) or an administrative rule adopted under Section 63F-1-206.

Section 6. Section 77-23c-105 is enacted to read:

77-23c-105. Exclusion of records.

All electronic information or data and records of a provider of an electronic
communications service or remote computing service pertaining to a subscriber or customer
that are obtained in violation of the provisions of this chapter shall be excluded subject to the
rules governing exclusion as if the records
were obtained in violation of the Fourth Amendment to the United States Constitution and