STAFF REPORT

DATE: June 18, 2019

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2019 Annual Surveillance Report, Cellebrite Universal Forensic Extraction Device

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Cellebrite Universal Forensic Extraction Device (CUFED) (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the CUFED (26.070.060 (b) DMC).
3. Make a determination that the continued use of the CUFED has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the CUFED and the existing use policy (Attachment 1).

Fiscal Impact

There is no fiscal impact to this report. If Council provides direction, future actions could have fiscal impacts.

Council Goal(s)

Goal 7 - Ensure a Safe and Healthy Community.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

2019 Annual Surveillance Report – CUFED

(a)The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;

CUFED was used to serve criminal search warrants on 33 devices for 13 felony investigations.

(2) A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

Information was shared with District Attorney and the issuing judges pursuant to the search warrant returns. Information was also properly discovered as required.

(3) A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the police department.

(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The use of the device is still the most effective way to access electronic information on a cell phone.

(6) Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Staff costs to operate the device and prepare reports.

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the CUFED Trackers *at the October 30, 2018, city council meeting. No other requests have been made.*

The City Council previously authorized use of the CUFED at the October 30, 2018, city council meeting. The staff report where the item was approved is attached to this staff report (Attachment 2). The information is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – CUFED
2. October 30, 2018, Staff Report to authorize use of CUFED

DAVIS POLICE DEPARTMENT

CELLEBRITE USE
Policy and Procedure 6.04-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Cellebrite Universal Forensic Extraction Device (CUFED) Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.

The CUFED is used to extract data from cell phones, smart phones or PDA's for use in criminal investigations.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.

The CUFED will be used to extract data from cell phones, smart phones or PDA's during criminal investigations via search warrant, written owner consent or when command staff has determined that exigent circumstances exist and that data must be extracted without delay (in these cases, a search warrant shall be secured within 3 days following the search as required by California Penal Code Part. 2, Title 12, Chapter 3.6).

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.

Data includes;

- Device Information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID (identifying device info.)
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and Picture Messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio Files
- Emails and Web Browsing Information (in some devices)
- GPS and Location Information (in some devices)
- Social Networking messages and contacts (in some devices)
- Deleted Data – Call Logs, Messages, Emails (in some devices)
- PIN Locked and Pattern Locked Bypass & Data Extraction – (on some devices – not all phones bypassed)
- Attached Media or memory card extraction (Pictures, files, app data – located on media card)
- Wireless (WI-FI) networks connected to the device (can assist in localizing a phone to a specific area)

(d) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

The CUFED can only be used by authorized police department personnel who are trained in its use and with approval of command staff when authorized by state and federal law.

(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

Data gathered by the CUFED is stored on a secure department server by downloading to a connected desktop computer. Data can then be printed hardcopy, loaded to a portable drive or burned to disc. All data is protected by password. The CUFED is secured in a locked area within the police building while phones and devices awaiting inspection are stored in the secured evidence room.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

(f) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

Extracted data is attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence when it is no longer needed or as required by the Electronic Communications Privacy Act or court order.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

All data is for the official use of the Davis Police Department.

Requests for data from the public or the media shall be processed in the same manner as requests for department public records.

Members of the public do not have access to this information when it is gathered as part of a criminal investigation; it is exempt from public disclosure pursuant to a public records request.

Data that is the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

Extracted data is generally only used by the Davis Police Department. However, extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

Individuals who operate the CUFED are trained in its use by department trainers and may also receive training directly from the vendor.

(j) Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

The use of the device is documented in a criminal police report. These devices are stored at the police department when not in use. A member is subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the use of the device. The review should include an analysis of the cost, benefit and effectiveness of the device, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: October 30, 2018

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – Cellebrite Universal Forensic Extraction Device

---

Recommendation

1. Hold a public hearing to consider the continued use of the Cellebrite Universal Forensic Extraction Device (CUFED) (26.070.030 (b) Davis Municipal Code (DMC)).
2. Make a determination that the continued use of the CUFED has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
3. Approve the continued use of the CUFED.
4. Adopt the proposed Surveillance Use Policy for the CUFED.

Fiscal Impact

There is no fiscal impact to this report. If Council provides direction, future actions could have fiscal impacts.

Council Goal(s)

Goal 7 - Ensure a Safe and Healthy Community.

Background and Analysis

Steps Required for Use of Surveillance Technology

Prior to adoption of the Surveillance Technology Ordinance (Article 26.07 DMC), the police department had access to a CUFED. The device is surveillance technology pursuant to 26.07.020 DMC.

A city department using surveillance technology prior to the effective date of the Surveillance Technology Ordinance shall submit a proposed **Surveillance Use Policy** no later than one hundred twenty days following the effective date of the ordinance for review and approval by the City Council (26.07.030 (a)(4) and 26.070.040 DMC).

The Surveillance Technology Ordinance was effective **May 3rd, 2018**. The deadline for a city department to submit staff reports noticing the required public hearings, **Surveillance Impact Reports** and **Surveillance Use Policies** to continue using existing technologies was **September 1, 2018**.

The police department is timely submitting this staff report, this **Surveillance Impact Report** and a proposed **Surveillance Use Policy.**

In order for the police department to continue using the CUFED, the following shall occur:

(1) **Public Notice –** The police department shall have submitted to the City Council a **Surveillance Impact Report** and a proposed **Surveillance Use Policy** via an informational staff report on a regular City Council meeting consent calendar at least thirty (30) days prior to holding a public hearing required under 26.07.030 (b) DMC. The informational staff report shall have been posted on the City website on a City Council agenda.

A **Surveillance Impact Report** means a written report including at a minimum the following:

(a) Information describing the surveillance technology and how it works, including product descriptions from manufacturers; and
(b) Information on the proposed purpose(s) for the surveillance technology; and
(c) If applicable, the location(s) it may be deployed and crime statistics for any location(s); and
(d) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public; and
(e) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding; and
(f) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis; and
(g) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.

A **Surveillance Use Policy** at a minimum specifies the following:

(a) The specific purpose(s) that the surveillance technology item is intended to advance.
(b) The uses that are authorized, and the rules and processes required prior to such use.
(c) The information that can be collected by the surveillance technology, including "open source" data.
(d) The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.
(e) The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal

vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the city.

(f) The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

(g) How collected information can be accessed or used by members of the public, including criminal defendants.

(h) If and how other city or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

(i) The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

(j) The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

Here, the police department submitted a **Surveillance Impact Report** and the proposed **Surveillance Use Policy** via an informational staff report on a regular City Council meeting consent calendar on **July 10, 2018**[1]. The public hearing being held pursuant to this staff report was scheduled for **August 28, 2018**, which is more than the 30-day notice requirement provided for under 26.070.030 (c) DMC.

The police department has received inquiries regarding the use of the technology and the proposed use policy since posting the material on the July 10, 2018, consent calendar (**see Attachment 1**)

(2) **Public Hearing** - A public hearing shall be held by the City Council in order to have an informed public debate about whether to continue using the surveillance technology.

(3) **Findings** - The City Council shall make a determination that the continued use of the CUFED has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city. The police department must obtain City Council approval following the public hearing to continue using the technology (26.07.030 (a)(3) DMC).

(4) **Policy Approval** - Council shall also review and approve the **Surveillance Use Policy** or the police department shall cease its use of the surveillance technology until such review and approval occurs, if ever (26.07.040 DMC).

[1]http://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180710/04M-1-Surveillance-Tech-Cellebrite.pdf

At the **August 28, 2018** meeting, the City Council opened the public hearing and continued it until **October 30, 2018**. At the **October 30, 2018** meeting, the City Council can **reject** the continued use of the CUFED, in which case the police department will **immediately stop** using the technology. The City Council may also approve, even on an interim basis, the use of the technology and the proposed **Surveillance Use Policy.**

Should the City Council neither reject nor approve the continued use of the technology and/or the **Surveillance Use Policy** at the **October 30, 2018**, meeting, the police department will be required to immediately stop using the device until such time as it is approved, if ever.

Surveillance Impact Report
Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

(a) Information on the proposed purpose(s) for the surveillance technology:
The CUFED is a forensic tool used to extract data from mobile phones, smartphones, and personal digital assistants (PDA's). The device itself is not surveillance technology. It simply extracts data from a device. However, because personal data is extracted, the use of the device raises constitutional privacy concerns that have been addressed by the United States Supreme Court (use requires search warrant, consent or exigent circumstances. Riley v. California (2014) 134 S. Ct. 2473).

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
The device is not deployed at a particular location. The CUFED is used at the police department. Personal technology devices such as smart phones are commonly used to commit crime and are commonly carried by those who commit crimes. These devices contain significant investigative data and the investigative data is used for criminal investigations and prosecutions.

(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;
Forensic extractions require a search warrant, written owner consent or exigent circumstances. The devices are commonly used by law enforcement agencies around the world. As with any other forensic device, extracted data must be carefully safeguarded to avoid releasing private information.

As specified by the Supreme Court in Riley v. California (2014) 134 S. Ct. 2473

> *Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated*

record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.

California Senate Bill 178 **was introduced and eventually passed (signed) in 2015**.

The legislative note stated - As introduced the bill would prohibit a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions, except for emergency situations, as defined.

The bill would also specify the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, or consent of the owner of the device. The bill would define a number of terms for those purposes, including, among others, “electronic communication information” and “electronic device information,” which the bill defines collectively as “electronic information.”

The bill would require a search warrant for electronic information to describe with particularity the information to be seized and would impose other conditions on the use of the search warrant or wiretap order and the information obtained, including retention, sealing, and disclosure. The bill would require a warrant directed to a service provider to be accompanied by an order requiring the service provider to verify by affidavit the authenticity of electronic information that it produces, as specified.

The bill would authorize a service provider to voluntarily disclose, when not otherwise prohibited by state or federal law, electronic communication information or subscriber information, and would require a government entity to destroy information so provided within 90 days, subject to specified exceptions. The bill would, subject to exceptions, require a government entity that executes a search warrant pursuant to these provisions to contemporaneously provide notice, as specified, to the identified target, that informs the recipient that information about the recipient has been compelled or requested, and that states the nature of the government investigation under which the information is sought.

The bill would authorize a delay of 90 days, subject to renewal, for providing the notice under specified conditions that constitute an emergency. The bill would require the notice to include a copy of the warrant or statement describing the emergency under which the notice was delayed. The bill would provide that any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of its provisions, according to specified procedures.

The bill would provide that a California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, wiretap order, or other order issued pursuant to these provisions.

According to the author:

> SB 178 updates California law to properly safeguard the robust constitutional privacy and free speech rights of Californians, spur innovation, and support public safety by instituting clear warrant standards for government access to electronic information.
>
> Californians must use technology every day to connect, work, and learn. The state's leading technology companies rely on consumer confidence in their services to help power California's economy. California law enforcement increasingly utilizes electronic information to protect public safety. The California legislature has long been a leader in enacting laws to properly balance the rights of Californians as technology advances. But California's statutory protections for electronic information is now very outdated.
>
> SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian's personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more. The California Supreme Court has long held that this type of information constitutes a "virtual current biography" that merits constitutional protection. SB 178 would codify that protection into statute. SB 178 also ensures that proper notice, reporting, and enforcement provisions are also updated and in place for government access to electronic information and to ensure that the law is followed.

Because the devices do contain detailed personal information, the devices themselves, when seized, must be securely stored as any other type of evidence used in criminal cases. Proper chain-of-custody must be maintained. Information shall only be extracted and shared pursuant to law (as discussed below).

(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

Initial Purchase Cost
$3,326.40 (already purchased).

Personnel Costs
Operator Certification - $850 – $2,000 (Cost ranges depending on software certification).

Ongoing Costs
None.

Potential Sources of Funding
Regular police department operating budget.

(e) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
There is no third party storage of data. Extracted data is stored locally on a secure police server and/or a removable drive so that it can be secured as any other digital evidence is. Data reports can be produced in hardcopy form or burned to DVD or thumb drive. Hardcopies are attached to criminal cases. DVD's and thumb drives are booked into evidence.

(f) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.
It is fairly common for officers to take phones at time of arrest and keep them as evidence either because the phone was used in the commission of a crime or there is probable cause to believe the phone contains evidence that may be used in the prosecution of a crime. A much smaller number of the phones that were taken are actually searched; most are simply returned to their owners when a person is released from custody or the case will not proceed beyond a preliminary investigative phase. The reason phones are generally seized early in an investigation is to avoid having the phone destroyed, information deleted and maintaining a strict chain-of-custody.

Phones are commonly used to facilitate crime or are used in the commission of a crime. Common crimes include homicide, stalking, sexual assault, harassing calls or texts, hate crimes, extortion, blackmail, fraud, sex trafficking, revenge porn, bullying, domestic violence, burglary/theft, robbery, drug sales/manufacturing and many others.

Phones and similar devices contain valuable information that is used in criminal prosecutions (pictures, texts, phone records, documents, GPS data). Phones may also contain exculpatory information or data that may clear a person from suspicion or is required to be discovered to the defense in a criminal case. Cell phone data can simply not be ignored in modern policing and investigative work because not only do the phones contain a wealth of information, but also because jurors expect to have physical data that links persons to criminal activity.

In Riley v. California (2014) 134 S. Ct. 2473 the United States Supreme Court ruled that, absent consent, in a vast majority of incidences a search warrant is required to search the contents of a phone (whether a Cellebrite device is used or not). This means, absent consent, in nearly all circumstances a phone search is conducted pursuant to a search warrant.

California has also enacted the Electronic Communications Privacy Act that further regulates phone searches and provides additional safeguards (California Penal Code Part. 2, Title 12, Chapter 3.6)[i].

Pursuant to both state and federal law, a phone may be searched with valid consent. Crime victims commonly consent to either a partial or complete search of their phone when the contents of the phone can aid in an investigation or the prosecution of a crime.

On rare occasions a criminal suspect will consent to a search of their phone; however, this is generally avoided because of the strong preference for using a search warrant in order to significantly reduce the possibility of suppression of evidence related to a warrantless search.

A government entity may also access electronic device information by means of physical interaction (e.g., looking through the phone) or electronic communication with the device (e.g., using Cellebrite) if the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information (Penal Code section 1546.1 (c)(6).

If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device (Penal Code section 1546.1 (h)).

The CUFED is a very common tool used by law enforcement all over the world for extracting data from cell phones, smart phones or PDA's. The device is effective in most cases. There are times when cell phone providers update and encrypt software so that the device cannot be accessed. In most, but not all, cases, the software on the CUFED can be updated so that data can be accessed. In order to extract data from devices, officers must have a search warrant or written consent.

Most certainly the improper release of extracted data may represent a significant violation of privacy. Also, phones contain significant information that may be unrelated to a criminal investigation.

In 2017 a Cellebrite external web server was hacked. The following was released by Cellebrite:

> *Cellebrite recently experienced unauthorized access to an external web server. The company is conducting an investigation to determine the extent of the breach. The*

impacted server included a legacy database backup of my.Cellebrite, the company's end user license management system. The company had previously migrated to a new user accounts system. Presently, it is known that the information accessed includes basic contact information of users registered for alerts or notifications on Cellebrite products and hashed passwords for users who have not yet migrated to the new system. To date, the company is not aware of any specific increased risk to customers as a result of this incident; however, my.Cellebrite account holders are advised to change their passwords as a precaution.

Cellebrite actively maintains an ongoing information security program and is committed to safeguarding sensitive customer information using best in class security countermeasures. Once the investigation of this attack is complete, the company will take any appropriate steps necessary to harden its security posture to mitigate the risk of future breaches.

Cellebrite is in the process of notifying affected customers. The company is working with relevant authorities regarding this illegal action and are assisting in their investigation.

The Davis Police Department had a Cellebrite device at the time of the incident and was not affected. Steps have been taken to maintain any downloaded media internally rather than externally.

The ACLU has also written about the Cellebrite device.

Mobile-Phone Cloning Tools Need to Be Subject to Oversight — and the Constitution
By Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy, and Technology Project
May 16, 2017

The claim by U.S. border officials that they can, with no grounds for suspicion, look through and copy travelers' cell phones and other electronic devices is creating justified consternation. But it's important to realize that police are also doing such searches domestically, sometimes without a warrant. Whether at the border or internally, the technology that is often used for those searches is called "mobile forensic data extraction devices"—portable machines that can download exact copies of a phone's entire memory. A company called Cellebrite is the most prominent maker of these devices; its products are sometimes described as the most advanced, and they are in wide use across U.S. law enforcement agencies.

This is an enormously powerful technology, and it needs to be subject to careful checks and balances. The use of these devices is already regulated by the Constitution, but additional protections ought to be enacted, ranging from tight internal law enforcement controls to prevent abuse, to close legislative monitoring and, if appropriate, regulation of law enforcement use.

The technology

Cellebrite and other mobile forensic extraction devices allow access to an enormously broad and intrusive range of data from cell phones. That information can include:

- *Call activity*
- *Phone book directory information*
- *Stored voicemails and text messages*
- *Photos and videos*
- *Apps*
- *Passwords*
- *Geolocation history, including cell towers and WiFi networks with which the cell phone has previously connected.*

Cellebrite boasts that its devices can download "hidden, and deleted phone data" including "call history, text messages, contacts, images, and geotags."

These devices also claim decryption capabilities. We don't know their precise limits, but it is safe to assume that the more advanced versions for sale have a state-of-the-art ability to break anything that it is poorly encrypted, where passwords are not strong (such as pins), or where software bugs not known to the public (so-called "zero-days") may allow it.

Furthermore, a Cellebrite product called "UFED Cloud Analyzer" allows police to access not only the information on a phone, but also all the information stored on cloud services, "utilizing login information extracted from the mobile device." Cellebrite boasts that this product can overcome "roadblocks and red tape by cloud service providers" (read: procedural safeguards and other checks and balances) and "provides forensic practitioners with instant extraction, preservation and analysis of private social media accounts."

Much of the extensive data that Cellebrite can access on a phone would be impossible for the government to obtain from a suspect's cellphone carrier.

These devices do not provide police access to a phone's data unless they can access the phone, either to plug in a cable or to accept a Bluetooth wireless connection on the phone. In other words, they cannot suck data off a phone remotely and in secret as is sometimes portrayed in television and the movies.

Need for a warrant for domestic use

Domestic cell phone searches should never be performed without a warrant based on probable cause. There is no difference between searching a cell phone and searching a personal computer, and the latter always requires a warrant. The Supreme Court has already ruled (in Riley v. California) that despite longstanding rules allowing police searches incident to arrest, the police may not search cell phones incident to arrest without a warrant because of the unprecedented amount of information now held on modern phones.

We have received reports that police in some places are routinely using Cellebrite without a warrant under the justification that the threat of remote wiping of seized phones constitutes an "exigent circumstance." This rationale does not hold water and was expressly rejected by the Supreme Court in Riley. Where police are worried about remote wiping they can, pending a warrant, simply put a phone inside a metallic "Faraday bag," which blocks all electromagnetic signals from reaching or emanating from the phone and thus prevents remote wiping or other alteration of a phone's content. (The police should have Faraday bags available for this purpose, but should they not have one they might be able to justify accessing a phone for the purpose of putting it into airplane mode.)

Like search warrants for desktop or laptop computers, any warrant to access a phone should particularly and narrowly describe the data that law enforcement have probable cause to believe is related to a crime. Just like a warrant for a person's business records in a fraud case shouldn't authorize police to look through their family photographs or medicine cabinet, a warrant looking for text exchanges with a particular number shouldn't allow police to look through photos or financial information stored on your phone, or in the cloud.

Nor should access through a phone to data stored in the cloud be carried out without specific, explicit authorization in a warrant.

Other points:

Searches should not be based on the fiction that consent from a citizen is "voluntary"—that individuals are free to refuse to cooperate with police officers asking to clone their cell phone data. Police officers have significant power and discretion in their encounters with civilians and few such police requests will be uncolored by coercion. Officers should be directed by policy not to make such requests.

Police should be open and transparent about their usage of and policies and practices with regard to this technology.

Some have proposed state laws creating an "implied consent" for cellphone searches in the aftermath of a serious automobile accident, so that the authorities can check whether use of a phone while driving contributed to an accident. This was proposed in the 2016 session in New York state as something called "Evan's Law," though the legislature did not pass it. The existing warrant framework is the proper way to approach such situations, and the ACLU opposes such laws.

At the Border

Customs and Border Protection claims the authority to search cell phones and seize data at the border for any reason or no reason at all—and is currently doing so—but we do not believe this is constitutional. It is true that customs officials have long had the power

to search through people's belongings. But people rarely cross international borders with a lifetime of personal paper correspondence, photographs, reading matter, purchase records, travel history, article clippings, audio recordings, videos, and personal writings in their possession. Yet people routinely carry such materials on their laptops and phones. The traditional powers of customs agents did not evolve based on that reality and as a result do not today adequately balance the government's need to exclude contraband with individuals' privacy rights.

Indeed, the Supreme Court accepted exactly this logic in Riley. That case is highly relevant to border searches because it also considered the limits of a longstanding government search power in light of the mega-storage capabilities of today's personal electronic devices. While the government protested that police had long had the power to search people when they are arrested, and therefore should not need a search warrant to search arrestees' cellphones, the Supreme Court said no. Writing for a unanimous court, Chief Justice John Roberts explained that

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick.

Roberts's last reference is to a previous case (U.S. v. Chadwick) that found that a 200-pound, locked footlocker could not be searched incident to arrest.

Part of the reason the Court ruled as it did in Riley is that it looked to the original purpose of the Fourth Amendment exception that had evolved. In the case of search incident to arrest, those purposes were to protect police officers from those who might be hiding a weapon later used to attack an officer or escape, and to prevent the destruction of evidence. Similarly, when it comes to border searches of U.S. citizens' devices we must remember the reason officials have the powers they do: to keep contraband goods out of the country. CBP officials have tried to frame the device-search issue in that light.

It is true there is such a thing as contraband data (such as child pornography), but it is very rare. More importantly, when it comes to CBP's stated goal of excluding illegal content from the United States, it seems silly to turn Americans' lives into an open book at the border so that CBP can search for digital contraband in their devices, when CBP rightly doesn't attempt (as it plainly lacks the authority) to examine all digital "goods" that cross our nation's borders via the Internet—in people's emails, downloaded from overseas web or FTP sites, etc. Checking data on devices while ignoring the Internet is like trying to monitor the trickle of water in a gutter while the Mississippi river flows nearby, unattended.

In reality, this issue isn't about CBP's right to search for and seize contraband goods at all. It's actually about border agents assuming sweeping new powers to peer into the lives of individuals crossing the border—to an extent agents have never been able to do in the past, especially for U.S. citizens, for whom admissibility is not at issue (all U.S. citizens having a right to return to their country) and contraband exclusion is the only possible rationale for searches.

In addition, insofar as CBP officials are now leveraging devices to search connected data held in the cloud, the "contraband exclusion" rationale is even weaker, because such data does not cross the border in any meaningful way. If I live in Virginia, and I upload photos to a cloud service provider based in California, why should customs be able to search those photos when I return from Paris? Similarly, if I live in Paris and am visiting the States, neither are my photos stored on servers in France crossing the border with me.

As we have argued in legal briefs, border searches of electronic devices using tools like Cellebrite should be permitted only with a warrant (or at a minimum, a demonstration of probable cause).

My colleagues have discussed border device searches in greater detail and offered advice for those entering or exiting the United States with electronic devices. We also offer an online form where anyone who has experienced a device search at the border can report their experience to us.

There is no doubt the use of the Cellebrite device is controversial. Almost 90% of adults have a cellphone and, as earlier discussed, cellphones contain enormous amounts of private information about people. Cellphones also often contain relevant information needed for criminal investigations and prosecution. The Electronic Communications Privacy Act regulates phone searches and provides mechanisms to safeguard privacy and protect information. (California Penal Code Part. 2, Title 12, Chapter 3.6). In enacting the legislation, California took a balanced approach to both secure private information and to allow for searches when a legal threshold is reached. Additionally, a judge has the authority to have information redacted from any official record if it is not relevant to a criminal case. The Davis Police Department follows the Electronic Communications Privacy Act.

Prior to the Davis Police Department acquiring direct access to a CUFED, devices were sent to other local and federal law enforcement agencies to extract information. That is no longer the case. However, should the Davis Police Department not be authorized to continue to use the department's CUFED, devices will again be sent to local and/or federal agencies to use a CUFED when authorized by judicial warrant. Alternatively, the Davis Police Department may simply not investigate crimes and/or prosecute crimes because the investigations would be constitutionally deficient if potentially exculpatory evidence was available, but not searched as allowed by state and federal law and disclosed as required by state and federal law.

The police department has not kept historical data on the number of times a CUFED has been used. Extraction reports have always been kept with individual police reports so they are not co-located. Use data will now be kept and reported as required by the Davis Surveillance Technology Ordinance.

Surveillance Use Policy

Council must adopt a policy at a regularly scheduled City Council meeting for use of the surveillance technology that at a minimum specifies the following:

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.

The CUFED is used to extract data from cell phones, smart phones or PDA's for use in criminal investigations.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.

The CUFED will be used to extract data from cell phones, smart phones or PDA's during criminal investigations via search warrant, written owner consent or when command staff has determined that exigent circumstances exist and that data must be extracted without delay (in these cases, a search warrant shall be secured within 3 days following the search as required by California Penal Code Part. 2, Title 12, Chapter 3.6).

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.

Data includes;

- Device Information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID (identifying device info.)
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and Picture Messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio Files
- Emails and Web Browsing Information (in some devices)
- GPS and Location Information (in some devices)
- Social Networking messages and contacts (in some devices)
- Deleted Data – Call Logs, Messages, Emails (in some devices)
- PIN Locked and Pattern Locked Bypass & Data Extraction – (on some devices – not all phones bypassed)
- Attached Media or memory card extraction (Pictures, files, app data – located on media card)
- Wireless (WI-FI) networks connected to the device (can assist in localizing a phone to a specific area)

(d) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

The CUFED can only be used by authorized police department personnel who are trained in its use and with approval of command staff when authorized by state and federal law.

(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

Data gathered by the CUFED is stored on a secure department server by downloading to a connected desktop computer. Data can then be printed hardcopy, loaded to a portable drive or burned to disc. All data is protected by password. The CUFED is secured in a locked area within the police building while phones and devices awaiting inspection are stored in the secured evidence room.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

(f) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

Extracted data is attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence when it is no longer needed or as required by the Electronic Communications Privacy Act or court order.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

All data is for the official use of the Davis Police Department.

Requests for data from the public or the media shall be processed in the same manner as requests for department public records.

Members of the public do not have access to this information when it is gathered as part of a criminal investigation; it is exempt from public disclosure pursuant to a public records request.

Data that is the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

Extracted data is generally only used by the Davis Police Department. However, extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

Individuals who operate the CUFED are trained in its use by department trainers and may also receive training directly from the vendor.

(j) Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

The use of the device is documented in a criminal police report. These devices are stored at the police department when not in use. A member is subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the use of the device. The review should include an analysis of the cost, benefit and effectiveness of the device, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

Oversight Following Initial Council Approval (26.07.060 DMC)

(a) By the end of each fiscal year, a City department that uses surveillance technology must present a written Annual Surveillance Report at a regular City Council meeting for City Council review for each approved surveillance technology item. If the City department is unable to meet the deadline, the department head shall notify the City Council in writing of staff's request to extend this period, and the reasons for that request. The City Council may grant reasonable extensions to comply with this Section.

(b) Based upon information in the Annual Surveillance Report, the City Council will, at a regular City Council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

"Annual Surveillance Report" means an annual written report concerning a specific surveillance technology.

(a) The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;

(2) A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

(3) A summary of community complaints or concerns about the surveillance technology item;

(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

(6) Statistics and information about any related Public Records Act requests;

(7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

(b) The Annual Surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes and/or information protected, restricted and/or sealed pursuant to State and/or federal laws, including information not required to be released by the Public Records Act.

Public questions and answers are attached. (Attachment 1)

Attachments

1. Public questions and answers

Attachment 1

"Cellebrite Universal Forensic Extraction Device (CUFED)":

1. Is it common for Davis PD to have a phone in their possession and decide not to seek a warrant to extract data? Please provide historical counts.

It is fairly common for officers to take phones at time of arrest and keep them as evidence either because the phone was used in the commission of a crime or there is probable cause to believe the phone contains evidence that may be used in the prosecution of a crime. A much smaller number of the phones that were taken are actually searched; most are simply returned to their owners.

Phones are commonly used to facilitate crime or are used in the commission of a crime. Common crimes include homicide, stalking, sexual assault, harassing calls or texts, hate crimes, extortion, blackmail, fraud, sex trafficking, revenge porn, bullying, domestic violence, burglary/theft, robbery, drug sales/manufacturing and many others.

Phones and similar devices contain valuable information that is used in criminal prosecutions. Phones may also contain exculpatory information or data that may clear a person from suspicion or is required to be discovered to the defense in a criminal case. Cell phone data can simply not be ignored in modern policing and investigative work.

Prior to the Davis Police Department acquiring direct access to a CUFED, devices were sent to other local and federal law enforcement agencies to extract information. That is no longer the case.

The police department has not kept historical data on the number of times a CUFED has been used. Extraction reports have always been kept with individual police reports so they are not co-located. Use data will now be kept and reported as required by the Davis Surveillance Technology Ordinance.

In Riley v. California (2014) 134 S. Ct. 2473 the United States Supreme Court ruled that, absent consent, in a vast majority of incidences a search warrant is required to search the contents of a phone (whether a Cellebrite device is used or not). This means, absent consent, in nearly all circumstances a phone search is conducted pursuant to a search warrant.

California has also enacted the Electronic Communications Privacy Act that further regulates phone searches and provides additional safeguards (California Penal Code Part. 2, Title 12, Chapter 3.6)[ii].

Pursuant to both state and federal law, a phone may be searched with valid consent. Crime victims commonly consent to either a partial or complete search of their phone when the contents of the phone can aid in an investigation or the prosecution of a crime.
On rare occasions a criminal suspect will consent to a search of their phone; however, this is generally avoided because of the strong preference for using a search warrant in order to significantly reduce the possibility of suppression of evidence related to a warrantless search.

A government entity may also access electronic device information by means of physical interaction (e.g., looking through the phone) or electronic communication with the device (e.g., using Cellebrite) if the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information (Penal Code section 1546.1 (c)(6).

If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device (Penal Code section 1546.1 (h)).

2. Given the broad nature of the data contained in a cell phone, what is Davis PD's procedure for determining when they should seek a warrant to extract data from a phone?

Both state and federal law govern the searches of phones. Phone searches are done in compliance with the law (see above).

3. What is Davis PD's procedure for determining and documenting if exigent circumstances justify extracting data from a cell phone without consent or a warrant?

There is a significant body of law that guides law enforcement on whether exigent circumstances exist, or not. Officers rely on that body of law, or case precedent, to aid them in determining whether they can conduct a warrantless search, or not.

As specified above, in those cases where there are exigent circumstances to initially justify a warrantless search, the officer is still required to comply with Penal Code section 1546.1 (h) and obtain a warrant within three days of conducting the search. This provides judicial review for all exigent circumstance searches.

4. Does a typical warrant give Davis PD access to all data on a particular cell phone or are they at times restricted to only accessing particular data (e.g. location data at a specific time)?

Pursuant to Penal Code Section 1536.1 (d) any warrant for electronic information shall comply with the following:

> (1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals

or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following (Penal Code section 1546.1 (e)):

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

5. Is there a procedure in place for an individual to give Davis PD consent to access some data on a cell phone (e.g. location data at a specific time), without giving Davis PD access to the entire contents of their phone?

Yes, a person granting consent can limit what they want searched and/or how they want the phone searched either verbally and/or in writing. Those limitations shall be followed. Searching the entire device requires consent to search the entire device. Consent can also be revoked at any time. If consent is revoked, any search that is already underway must immediately stop. The Cellebrite device is not used in all phone searches. Searches are often done by looking through the device and screenshotting documents for electronic transfer and printing.

6. Will the annual report include the number of times used by misdemeanor and felony charges? Annual impact report should quantify number of times CUFED has been used

in prior 12 months, under what authority (warrant, written owner consent, exigent circumstances, and if warrant was obtained within 3 days).

As specified in the ordinance, the Annual Surveillance Report submitted to the City Council will include all of the following:

1. A general description of how the surveillance technology was used;

2. A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

3. A summary of community complaints or concerns about the surveillance technology item;

4. The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

5. Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

6. Statistics and information about any related Public Records Act requests;

7. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

8. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

9. Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

10. A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

11. The Annual Surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes and/or information protected, restricted and/or sealed pursuant to State and/or federal laws, including information not required to be released by the Public Records Act.

7. How are removable data storage devices with extracted data tracked and destroyed when no longer needed for a prosecution?

Destruction is in compliance with state law. Items are destructed in such a manner they are no longer usable. Crime report evidence sheets are used to track the location/destruction of evidence.

8. How does the owner of the phone and his/her counsel access the data? They are the first party, not the third party. This is not addressed in the policy.

Through the criminal discovery process governed by state and federal law.

9. Why do the auditing and oversight mechanisms not specify review by the Independent Police Auditor and the Davis Police Accountability Commission? We request that this be added.

The ordinance specifies the Council will receive the Annual Surveillance Report. However, the reports will be shared with the Auditor and Commission (The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies).

---

[i] **CHAPTER 3.6. Electronic Communications Privacy Act [Penal Code 1546 - 1546.4]**

1546

For purposes of this chapter, the following definitions apply:

(a) An "adverse result" means any of the following:

(1) Danger to the life or physical safety of an individual.

(2) Flight from prosecution.

(3) Destruction of or tampering with evidence.

(4) Intimidation of potential witnesses.

(5) Serious jeopardy to an investigation or undue delay of a trial.

(b) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(c) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

(d) "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "Electronic communication information" does not include subscriber information as defined in this chapter.

(e) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

(f) “Electronic device” means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver’s license or an identification card issued by this state or a driver’s license or equivalent identification card issued by another state.

(g) “Electronic device information” means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

(h) “Electronic information” means electronic communication information or electronic device information.

(i) “Government entity” means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(j) “Service provider” means a person or entity offering an electronic communication service.

(k) “Specific consent” means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

(l) “Subscriber information” means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

1546.1

(a) Except as provided in this section, a government entity shall not do any of the following:

(1) Compel the production of or access to electronic communication information from a service provider.

(2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.

(b) A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.

(4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(5) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to a tracking device search warrant issued pursuant to paragraph (12) of subdivision (a) of Section 1524 and subdivision (b) of Section 1534.

(4) With the specific consent of the authorized possessor of the device.

(5) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

(6) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

(7) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the government entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

(8) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility or a secure area of a local detention facility where inmates have access, the device is not in the possession of an individual, and the device is not known or believed to be the possession of an authorized visitor. This paragraph shall not be construed to supersede or override Section 4576.

(9) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is serving a term of parole under the supervision of the Department of Corrections and Rehabilitation or a term of postrelease community supervision under the supervision of county probation.

(10) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release.

(11) If the government entity accesses information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.

(12) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(d) Any warrant for electronic information shall comply with the following:

(1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is

probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.

(h) If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.

(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

(3) Require a service provider to provide subscriber information.

(j) This section does not limit the authority of the Public Utilities Commission or the State Energy Resources Conservation and Development Commission to obtain energy or water supply and consumption information pursuant to the powers granted to them under the Public Utilities Code or the Public Resources Code and other applicable state laws.

(k) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity's possession.

1546.2

(a) (1) Except as otherwise provided in this section, any government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other

means reasonably calculated to be effective, the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been compelled or obtained, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three court days after obtaining the electronic information.

(2) Notwithstanding paragraph (1), notice is not required if the government entity accesses information concerning the location or the telephone number of an electronic device in order to respond to an emergency 911 call from that device.

(b) (1) When a warrant is sought or electronic information is obtained in an emergency under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant or emergency access, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(c) If there is no identified target of a warrant or emergency access at the time of its issuance, the government entity shall submit to the Department of Justice within three days of the execution of the warrant or issuance of the request all of the information required in subdivision (a). If an order delaying notice is obtained pursuant to subdivision (b), the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b). The department shall publish all those reports on its Internet Web site within 90 days of receipt. The department may redact names or other personal identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

1546.4

(a) Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to review

in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5.

(b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter.

(c) An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.

(d) A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.

[ii]**CHAPTER 3.6. Electronic Communications Privacy Act [Penal Code 1546 - 1546.4]**

1546

For purposes of this chapter, the following definitions apply:

(a) An "adverse result" means any of the following:

(1) Danger to the life or physical safety of an individual.

(2) Flight from prosecution.

(3) Destruction of or tampering with evidence.

(4) Intimidation of potential witnesses.

(5) Serious jeopardy to an investigation or undue delay of a trial.

(b) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(c) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

(d) "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "Electronic communication information" does not include subscriber information as defined in this chapter.

(e) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

(f) "Electronic device" means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver's license or

an identification card issued by this state or a driver's license or equivalent identification card issued by another state.

(g) "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

(h) "Electronic information" means electronic communication information or electronic device information.

(i) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(j) "Service provider" means a person or entity offering an electronic communication service.

(k) "Specific consent" means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

(l) "Subscriber information" means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

1546.1

(a) Except as provided in this section, a government entity shall not do any of the following:

(1) Compel the production of or access to electronic communication information from a service provider.

(2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.

(b) A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.

(4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(5) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to a tracking device search warrant issued pursuant to paragraph (12) of subdivision (a) of Section 1524 and subdivision (b) of Section 1534.

(4) With the specific consent of the authorized possessor of the device.

(5) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

(6) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

(7) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the government entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

(8) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility or a secure area of a local detention facility where inmates have access, the device is not in the possession of an individual, and the device is not known or believed to be the possession of an authorized visitor. This paragraph shall not be construed to supersede or override Section 4576.

(9) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is serving a term of parole under the supervision of the Department of Corrections and Rehabilitation or a term of postrelease community supervision under the supervision of county probation.

(10) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release.

(11) If the government entity accesses information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.

(12) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(d) Any warrant for electronic information shall comply with the following:

(1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.

(h) If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.

(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

(3) Require a service provider to provide subscriber information.

(j) This section does not limit the authority of the Public Utilities Commission or the State Energy Resources Conservation and Development Commission to obtain energy or water supply and consumption information pursuant to the powers granted to them under the Public Utilities Code or the Public Resources Code and other applicable state laws.

(k) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity’s possession.

1546.2

(a) (1) Except as otherwise provided in this section, any government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been

compelled or obtained, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three court days after obtaining the electronic information.

(2) Notwithstanding paragraph (1), notice is not required if the government entity accesses information concerning the location or the telephone number of an electronic device in order to respond to an emergency 911 call from that device.

(b) (1) When a warrant is sought or electronic information is obtained in an emergency under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant or emergency access, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(c) If there is no identified target of a warrant or emergency access at the time of its issuance, the government entity shall submit to the Department of Justice within three days of the execution of the warrant or issuance of the request all of the information required in subdivision (a). If an order delaying notice is obtained pursuant to subdivision (b), the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b). The department shall publish all those reports on its Internet Web site within 90 days of receipt. The department may redact names or other personal identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

1546.4

(a) Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5.

(b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter.

(c) An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.

(d) A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.