LEGAL ISSUES IN SEARCHING CELL PHONES AND OTHER ELECTRONIC DEVICES

Kristine M. Knowlton, Assistant Utah Attorney General, Section Chief ICAC Prosecution and CNS sections

Basic premise – citizen has reasonable expectation of privacy in home, person and property

Government access requires: warrant; consent; or exception to warrant

Cell phones and other similar devices are the tools of the modern criminal

- Can be used to store evidence of crime
- Can also be used as instrumentality of crime: plan; commit; even record crime
- Been described as "virtual biographers of our daily activities"

WHEN YOU WANT TO KNOW WHAT DEVICE CONTAINS

WARRANT

- When there's time to do so, should always get a warrant
- Special considerations when want to <u>search</u> cell phone
    - You want to search for and obtain the DATA that is <u>evidence of a crime</u> (what kinds of data: think about images, contact lists, text messages, emails, videos, calendars, appointments, Apps, websites, search terms, accounts, user names, etc)
        - The phone is simply the container
            - holding the contraband
            - holding the evidence related to the crime such as records, address books, call logs, photos
        - Focus on <u>data</u> you want that is evidence of a crime

        - Then request warrant for authorization to search anywhere that data might be found, including cell phone, computers, etc.
    - This way not limiting yourself in a residential search warrant to search just for a cell phone or just for a computer…it is for any place your articulated data evidence may be found
- Is it an Instrumentality of crime?
- Probable cause considerations
    - Calls to or from target to witness, CI
    - Texts
    - Call logs
    - Articulate knowledge that cell phones are often used in commission of crime: used by lookouts; used to arrange mtg times and places for "customers"
    - Articulate that suspects may take photos to plan their crimes…photos of security devices, surveillance cameras, guard posts
    - Articulate that it's not unusual for suspects to take photos, send text messages or emails (especially anonymous texts or emails or fake user names and in cases of throw away phones where officer cannot track phone number to specific subscriber) in stalking and harassment cases
    - Others may take videos or other pictures of themselves actually committing the crime

CONSENT

- May be limited in scope
    - Ex: consent to look at phone logs and while looking, officer sees child pornography; officer seizes phone as evidence of crime and then applies for SW using the

information he saw to search for other evidence, data re: the crime of CP

- May be revoked
    - If officer has already recognized evidence of a crime on a phone and suspect revokes consent, officer can seize phone to prevent destruction of that data and evidence under exigent circumstances

EXCEPTIONS TO WARRANT

- **Exigent circumstances**
    - When officer has PC there is evidence of a crime and that evidence might be immediately destroyed, it is reasonable to seize the evidence or the container it is in to prevent its destruction. If search of evidence or container also necessary to prevent destruction, then searching also permissible
        - If officer can articulate that it's possible that the data on a phone can be remotely deleted and that the phone has been lawfully seized, the phone can also be searched w/o a warrant
        - See ***US v Wurie*** 1st Cir No 11-1792, 5/17/2013, where police seized cell phone from an individual's person as part of his lawful arrest and then searched the phone's data without a warrant. Court held the search of the data exceeded "the boundaries of the Fourth Amendment search-incident-to-arrest exception". Because the government didn't argue "that the search was justified under 'exigent circumstances' or any other exception", (such as necessity to prevent immediate destruction), denial of motion to suppress was reversed, conviction vacated and case remanded to district court.
            - August 2013, govt filed petition asking Supreme Court to hear case, arguing 1st Cir ruling conflicts with several other appeals courts and earlier SCt cases which have

given police broad discretion to search possessions on person of arrested person and that cell phone is no different than any other object suspect might be carrying

- Public safety and safety of officer. see ***US v Lottie***, 2008 WL 150046 at 3 (unpublished) where counter-surveillance caused concern for officer safety and for the public in the midst of a large drug transaction and entitled officers to immediately search cell phone.

- **Mobile conveyance**
  - If a car is readily mobile and PC exists to believe it contains contraband or evidence of the commission of a crime, the 4th Amendment permits the police to search the vehicle as well as containers in the vehicle (***Carroll v US*** 267 US 132 (1925), ***Pennsylvania v Labron***, 518 US 938 (1996)
  - While an electronic communication device (laptop, cell phone, etc.), has been considered a "container" by courts, it has also been compared more to a file cabinet than a purse, because of the immense amount of data, documents, personal medical info it can hold; therefore best practice is to obtain a warrant to search for the contents of the "container".
  - In ***US v Rocha***, 2008 WL 4498950, officers searched vehicle after traffic stop and found drugs and four cell phones. Detective recovered contact lists, numbers dialed and recent calls from each phone w/o warrant. The court held that "because probable cause existed to believe that evidence of a crime would be found in the cell phone information, the automobile exception allows the search of the cell phone just as any other closed container".

- **Inventory**
  - LE must have standard inventory policy specifically addressing search of electronic devices in order to justify searching cell phone, etc; other search would be beyond scope of inventory

- **CAVEAT**: even if agency had policy re: data searches, it probably would be unconstitutional as purpose of inventory is to protect property taken by the govt.
- Also may put data at risk by turning on device to inventory data
- ***U.S.* v. *Wall***, 2008 U.S. Dist. LEXIS 103058, 10 (S.D. Fla. 2008).
    - The court recognized that a cell phone may be identified as an item seized during a post arrest inventory. "However, there is no need to document the phone numbers, photos, text messages, or other data stored in the memory of a cell phone to properly inventory the person's possessions because the threat of theft concerns the cell phone itself, not the electronic information stored on it"

- **Search Incident to Arrest (SIA)**
    - ***US v Finley*,** 477 F3d 250 (5th Cir.2007), leading example of permissible cell phone search incident to arrest, analogizing a cell phone to a closed container
        - Other courts have declined to follow *Finley* . ***US v Park,*** 2007 WL 1521573 (unpublished), The Northern District of California court explained it was "unwilling…to authorize the warrantless search of contents of cellular phone" ; that the quantity and quality of information contained in an electronic device distinguishes it from other physical containers or items such as wallets and diaries. Court did note that no evidence had been given that search of phone was caused by concern for officer safety or to prevent the concealment or destruction of evidence. (case cited by Tenth Circuit in ***US v Gutierrez***, 2008 WL 2397668.)
    - ***Arizona v Gant***, 556 US 332 (2009), the US SCt held that police may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest. "Under ***Chimel***, 395 US 752 (1969),

police may search incident to arrest only the space within an arrestee's " 'immediate control,' " meaning "the area from within which he might gain possession of a weapon or destructible evidence." 395 U. S., at 763. The safety and evidentiary justifications underlying *Chimel*'s reaching-distance rule determine *Belton*'s scope. Accordingly, we hold that ***Belton**, 453 US 454 (1981),* does not authorize a vehicle search incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle. Consistent with the holding in ***Thornton* v. *United States***, 541 U. S. 615 (2004) , and following the suggestion in Justice Scalia's opinion concurring in the judgment in that case, *id.*, at 632, we also conclude that circumstances unique to the automobile context justify a search incident to arrest when it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle

- ***Silvan W.* v. *Briggs*** is a unique case. It is an unpublished decision in a civil rights lawsuit alleging, among other causes of action, that the warrantless search of a cell phone incident to arrest was a Fourth Amendment violation. Officers responded to allegations of sexual abuse of a minor. Two family members were arrested for obstruction of justice, cell phone seized from person incident to arrest and a cell phone's address book was searched incident to arrest in an attempt to learn the location of the abused child. The 10th Circuit held that the search was lawful and dismissed the suit. 2009 U.S. App. LEXIS 1520 (10th Cir. 2009) (unpublished; facts available at 2009 WL 159429).
- Officer must be able to articulate that evidence in cell phone is destructible thus necessitating immediate search
    - Cell phones almost always have finite memory; impacts size of call logs as well as # of text messages it can hold; new calls or texts could replace older texts and calls, thereby bumping the older data from the phone before a search warrant could be obtained

        - Also owner can arrange for remote access by another person to delete the data, even when the phone is in the hands of the police
        - Courts have gone both ways ion this issue
        - Best case is for officer to articulate both an SIA and an exigent circumstance to search cell phone for data…but remember, must have PC that evidence is on phone to support exigent circumstance exception (immediate destruction; vehicle exception) which is not necessary in SIA
        - SIA must also be substantially contemporaneous to the arrest
        - See ***US v Parada***, 289 F.Supp.2d 1291 (D.Kansas 2003)

- **Inevitable Discovery**
    - ***US v Morales-Ortiz*****,** 376 F.Supp.2d 1131 (D.N.M. 2004). DEA agents executed arrest warrant for defendant at his residence. While conducting protective sweep, they found a pager and searched thru the messages as well as searched thru numbers found in a cell phone. Search warrant then obtained for residence, authorizing seizure of pager and cell phone. Court held even tho' originally unlawfully searched, the contents still admissible under inevitable discovery as pager and cell phone would have been searched legally pursuant to search warrant.

WHEN YOU WANT TO KNOW WHERE CELL PHONE HAS BEEN

- Emergency circumstance in cases of kidnapping, etc.
    - Exigent circumstance exception
    - Emergency Aid Doctrine exception or Community Caretaker exception where primary purpose is the health or safety of individual
        - police must have reasonable grounds to believe emergency exists
        - entry into home/car must be reasonable attempt to protect life, safety

        - scope of search must be related to protection, preservation of life
        - ***Brigham City, UT v Stuart*** USSCt 2006
- Business records exception
    - 5th Circuit US Court of Appeals case, ***In Re: Application of the United States of America for Historical Cell Site Data,*** says warrantless search for historical data directly from communications carrier constitutional as location was "clearly a business record" and therefore not protected by the 4th Amendment but governed by federal ***Stored Communications Act 18 USC § 2793.***
    - The government has the right to conduct warrantless searches of such business records, which are created by phone companies (third party doctrine) for billing customers for phone use, according to the ruling. The federal Stored Communications Act requires the standard of "specific and articulable facts" by LE to obtain order for that data which enables the judicial branch to prevent and remedy executive overreaching. ***In Re: Application of the United States of America for Historical Cell Site Data***, 11-20884, July 30, 2013, U.S. Court of Appeals for the Fifth Circuit (New Orleans); cases in two other circuits are pending.

- Get search warrant otherwise
    - Cell tower pings
    - Call origination
    - Call termination
    - Victim phone/ suspect phone

WHEN YOU WANT TO KNOW WHO THE SUBSCRIBER OF THE SERVICE IS

- Administrative subpoena – §77-22-2.5
    - Can be used only for investigations involving sexual offense against a minor, stalking and child kidnapping
    - Can only obtain subscriber info, NOT CONTENT

        - Names; addresses; local and long distance telephone connections; records of session times and duration; length of service, including start date and types of services utilized; telephone or other instrument subscriber numbers or other subscriber identifiers, including temporarily assigned network addresses; and means and source of payment for the service, including credit card or bank account numbers.
    - Statute specifies non-disclosure by provider to subscriber §77-22-2.5(5);
    - Govt not required to provide notice to subscriber §77-23b-4(3)(b)
- Search Warrant for Third Party (service provider)
    - Rule 40(c)(2), URCrP
        - If the item sought to be seized is evidence of illegal conduct, and is in the possession of a person or entity for which there is insufficient probable cause shown to the magistrate to believe that such person or entity is a party to the alleged illegal conduct, **no search warrant shall issue except upon a finding by the magistrate that the evidence sought to be seized cannot be obtained by subpoena, or that such evidence would be concealed, destroyed, damaged, or altered if sought by subpoena**. If such a finding is made and a search warrant issued, the magistrate shall direct upon the warrant such conditions that reasonably afford protection of the following interests of the person or entity in possession of such evidence: protection against unreasonable interference with normal business; protection against the loss or disclosure of protected confidential sources of information; or protection against prior or direct restraints on constitutionally protected rights.
    - Notice provision applies: §77-23b-6(1)(e)

WHEN YOU WANT TO KNOW CONTENTS OF THE COMMUNICATION S

- Search Warrant
    - Delay in notification by provider and govt to subscriber §77-23b-6(1)(a)
        - Not to exceed 90 days; may get extension up to add'l 90 days
        - Written certification of supervisory official that there is reason to believe notification of existence may have adverse result
    - Delay in notification to subscriber by government
    - Notice provision – §77-23b-6(1)(e)
        - Copy of process
        - Plus notification/certification letter

IMPORTANT TO READ BOTH Title 77, chapter 23b and Title 77, Chapter 22, section 2.5 when dealing with electronic communications