*Amendment IV*

*The right of the people to be secure in their persons, houses, papers, and effects, against* ***unreasonable*** *searches and seizures, shall not be violated, and* ***no warrants*** *shall issue,* ***but upon probable cause****, supported* ***by oath or affirmation****, and* ***particularly*** *describing the place to be searched, and the persons or things to be seized.*

1. Fourth Amendment
   1. Reasonable expectation of privacy is subjective but must be reasonable
      1. *Kyllo v. US,* 533 U.S. 27, 33 (2001) (expectation of privacy is “subjective” and one “that society recognizes as reasonable.”)
      2. *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (a defendant “must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable.”)
      3. *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (defendant had no reasonable expectation of privacy when marijuana plants were visible from plane overhead; expectation only extended to physical intrusions).
   2. Thus, a Defendant cannot assert the Fourth Amendment rights of another. He or she lacks standing to do so.

i. *US v. Salvucci*, 488 U.S. 83, 85 (1980).

* 1. Expectation of privacy in the home and its curtilage
     1. *Silverman v. US*, 365 U.S. 505, 511 (1961) (“At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. This Court has never held that a

federal officer may without warrant and without consent physically entrench into a man’s office or home, there secretly observe or listen, and relate at the man’s subsequent criminal trial what was seen or heard.”)

* + 1. *Minnesota v. Olson*, 495 US 91, 98 (1990) (Expectation of privacy extends to *overnight* guests).
    2. *Minnesota v. Carter*, 525 US 83, 90 (1998) (But expectation of privacy does not extend to mere guests).
    3. *Stoner v. California*, 376 U.S. 483 U.S. 490 (1964) (Expectation of privacy extends to hotel rooms).
    4. But, there is no reasonable expectation of privacy in private property adjacent to the home that is not “curtilage” and is, instead, an “open field.” *Oliver v US*, 466 U.S. 170 (1984).

1. Exceptions to Warrant Requirement
   1. Search Incident to Arrest
      1. *Chimel v. California*, 395 U.S. 752 (1969) (allows officers to search in areas where an arrestee might grab a weapon or destroy evidence).
      2. *New York v. Belton*, 453 U.S. 454 (1981) (permits a search of a passenger compartment of a vehicle)
      3. *Arizona v. Gant*, 556 U.S. 332 (2009) (search of vehicle must be close in time or there must be indication that car contains evidence of the offense).
   2. Exigent Circumstances
      1. Does not apply if officers have enough time to get a warrant. *Missouri v. McNeely*, 133 S. Ct. 1552, 1572 (2013).
      2. But applies during emergency: *Brigham City, Utah v. Stuart*, 547 U.S. 398 (2006) (officers can enter a home if they believe they can prevent imminent injury).
      3. And applies if officers are in hot pursuit: *Kentucky v. King*, 131 S. Ct. 1849 (2011) (officers can enter premises when in hot pursuit).
   3. Automobiles
      1. No warrant requirement, but car searches do require probable cause and the scope of the search must be related to the items for which there is probable cause. *US v. Ross*, 456 U.S. 798.
   4. Inventory Searches
      1. No warrant necessary to search a seized vehicle to inventory its contents.

*Florida v. Wells*, 495 U.S. 1 (1990)

* + 1. But inventory must be conducted according to established procedures.

*Illinois v. Lafayette*, 462 U.S. 640 (1983).

* 1. Consent
     1. Consent must be freely and voluntarily given and “not the product of duress or coercion, express or implied.” *Schneckloth v. Bustamonte*, 412 U.S. 218, 228 (1973)
     2. However, submission to lawful authority is not consent. *Kaupp v. Texas*, 538 U.S. 626, 631 (2003).
     3. Person who gives consent must have authority to do so. *US v. Matlock*, 415 U.S. 164 (1974)
  2. Plain view
     1. Predicated on notion that there is no expectation of privacy in something that is in plain sight.
     2. The illegal nature of the object must be readily apparent and "the officer [must] be lawfully located in a place from which the object can be plainly seen, but he or she must also have a lawful right of access to the object itself.” *Horton v. California*, 496 U.S. 128, 137 (1990)
     3. *Arizona v. Hicks*, 480 U.S. 321 (1987) (because officers had to move stereo to determine that it was stolen, it was not in plain view).
  3. Border Searches
     1. No requirement of a warrant *or* probable cause at any port of entry or its functional equivalent, including international airports. *US v. Flores- Montano*, 541 U.S. 149 (2004).
     2. But search must be reasonable. “We again leave open the question ‘whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner it is carried out.’” *Flores-Montano*, 541 U.S. at 154 n.2. (citing US v. Ramsey, 431 U.S. 606, 618, n. 13 (1977)
  4. Parole & Probation Searches
     1. Search of probationer’s home based on reasonable suspicion not unreasonable. *US v. Knights*, 534 U.S. 112 (2001).
     2. Parolees have diminished expectations of privacy so warrantless searches of homes permissible. *Samson v. California*, 547 U.S. 843, 857 (2006)

1. Challenging a Warrant
   1. A warrant must be supported by probable cause set out in an affidavit sworn under oath. Probable cause requires “a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983).
   2. Search warrants must particularly describe the places and items to be searched. *Kentucky v. King*, 563 U.S. 452, 459 (2011) (requiring scope of search to be “set out with particularity.”)
      1. Purpose of particularity requirement is to make general searches impossible and to give officers specific information about what can be searched. *Marron v. US*, 275 U.S. 192 (1927).
      2. If the search exceeds the scope of the search warrant, it is unconstitutional.

*Horton v. California*, 496 U.S. 128 (1990).

* 1. Nexus requirement: There must be a relationship between the items sought and the areas to be searched. *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).
  2. Information in a search warrant affidavit must not be too stale. *US v. Grubbs*, 547 U.S. 90, 95 n.2 (2006).
  3. Search warrant must be based on truthful information. *Franks v. Delaware*, 438

U.S. 154, 156 (1978) (A search warrant may be invalid if it is based on “a false statement knowingly and intentionally, or with reckless disregard for the truth.”). The remedy for a *Franks* violation is to excise the offending information and re- evaluate probable cause in light of the excised information. *Id.* at 171-172.

1. The Exclusionary Rule: The long-standing principle that illegally-obtained evidence is inadmissible against a criminal defendant. *Wong Sun v. US*, 371 U.S. 472 (1963).
   1. But the Supreme Court is pushing back against the use of the exclusionary in every instance of a Fourth Amendment violation. *Davis v. US*, 131 S. Ct. 2419, 2427 (2009) (“deterrence benefits of suppression must outweigh its heavy costs.”); *See also Herring v. U.S.,* 555 U.S. 135 (2009).
   2. For exclusionary rule to apply, the taint of the illegal search or search cannot be so attenuated as to dissipate the taint. *Segura v. US*, 468 US 796 (1984).
   3. Exclusionary rule does not apply if evidence would have been “inevitably discovered.” *Nix v. Williams*, 467 U.S. 431 (1984).
   4. Exclusionary rule does not apply if evidence was obtained lawfully through, “an independent source.” *Murray v. US*, 487 US 533 (1988).
2. The Good Faith Exception to the Exclusionary Rule
   1. Even if a warrant is invalid, the exclusionary rule does not apply if officers had good faith. *US v. Leon*, 468 U.S. 897 (1984).
      1. But good faith does not apply if officers are dishonest in the application for a search warrant. *See Franks v. Delaware*, 438 U.S. 154 (1978) (cited above).
      2. Court authorizing warrant must be neutral and not merely a rubber stamp.

*Leon*, 468 at 923.

* + 1. Warrant can be so facially deficient that officers cannot reasonably rely on it. *Id.*

*Sample Motion Challenging Search of Electronic Data*

# I. INTRODUCTION

The Fourth Amendment prohibits general search warrants and requires that a warrant describe, with particularity, the place to be searched and the persons or things to be seized. The United States sought and obtained broad warrants to search nearly the entirety of the following, 1) three Google accounts, 2) Facebook account, 3) a Dell Inspiron laptop, and 4) five digital devices. The fruits of the warrants should be suppressed because the warrants lacked probable cause and were not sufficiently particular, in what was to be searched, how it was to be searched, and over what time periods. These searches violate the Fourth Amendment. The government should have provided the court the methods and procedures that the government would use to look in limited areas of the accounts and electronic devices for limited information.

Instead, the warrants allowed the government to rummage through Mr. X’s entire electronic history sifting for evidence. The types of general warrants authorized by the magistrates in this case, have never been permitted in the history of the United States.

# II. STATEMENT OF FACTS

After suspecting Mr. X of engaging in sex-trafficking, the United States sought and obtained a general warrant to rummage through Mr. X’s three Google accounts, Facebook account, and his Dell Inspiron personal computer. After arresting him for sex trafficking, the government sought a general warrant to rummage through five more of his digital devices.

Mr. X is charged in the indictment of committing illegal acts from September 2014 through January 2015. The warrants sought information from his Google and Facebook accounts back to July 2014. The warrants for the information on the six electronic devices were without time limitations.

The results of these warrants produced thousands upon thousands of pages of information.

# The magistrate judges issue broad warrants

On February 10, 2015, Magistrate Judge Diana Prince signed three warrants in this case. First, Google was ordered to produce all information in its possession regarding three email accounts

associated with Mr. X from the overbroad time period. *See* Ex. A, Google Warrant at Page 18, Paragraph 24 (“I request authority to seize all content”). Second, Facebook was ordered to produce all information in its possession regarding Mr. X’s account with them from the overbroad time period. *See* Ex. B, Facebook Warrant at Page 13, Paragraph 50 (“I request authority to seize all content”). Third, the magistrate issued a warrant to search through the entire contents of Mr. X’s personal computer, a Dell Inspiron 15. *See* Ex. C, Dell Inspiron Warrant at page 18, paragraph d. (requesting permission to create a forensic image (“A forensic image is an exact physical copy of the hard drive or other media.”))

On April 1, 2015, Magistrate Judge Draco Malfoy signed a warrant. This warrant authorized the search of five electronic devices seized on the day of Mr. X’s arrest. *See* Ex. D, Electronic Devices Warrant at Page 29. The warrant sought permission to search the entire contents of the five phones by creating a forensic image if possible. *See id.* at page 23, paragraph d. (requesting permission to create a forensic image (“A forensic image is an exact physical copy of the hard drive or other media.”)

# The Google warrant request for all account information

As stated above, Google was ordered to produce all information in its possession regarding three email accounts associated with Mr. X back to July 2014. *See* Ex. A, Google Warrant at Page 18, Paragraph 24 (“I request authority to seize all content”).

The complete and voluminous results from Google were supposed to be searched according to “Procedures for Electronically Stored Information.” Ex. A, Attachment B, Page 22. However, no procedures for searching the accounts for relevant evidence were actually described. Ex. A, Affidavit, Page 17-19. Rather, the application simply explained that searching email is complicated and time-consuming. The lack of protocols resulted in the search of Mr. X’s entire Google accounts with the “relevant data” being extracted and saved in a new location.

Some of the Google accounts data searched by the government include:

* Photos of him at the Universal Studios amusement park;
* Photos of sea lions laying on the sand at the beach;
* Metadata of the photos including the time and date photos were created;
* It includes date that email address was created;
* It includes other email addresses associated with the email account;
* It included IP addresses and the time that computers accessed the account in hundreds of instances;
* It included Mr. X’s perhaps 100 different contacts including “[verification@diapers.co](mailto:verification@diapers.co)” and “Greg Pizza.”
* It included emails from dental insurance companies, Target.com, and the Lasik vision institute.

The warrant application authorized the search and seizure of this data, but it is not in any way relevant to the charges against Mr. X. The lack of particularity and procedures set forth in the warrant application resulted in an over-breadth of seized and searched materials which have nothing to do with the crimes investigated or charged.

# The Facebook warrant request for all account information

Facebook was ordered to produce all information in its possession for the account associated with Mr. X from July 2014 to January 2015. *See* Ex. B, Facebook Warrant at Page 13, Paragraph 50 (“I request authority to seize all content”). The warrant application requested permission to seize the following information:

* + - All subscriber and/or user information, including personal identifying information, full name, user identification number, birth date, gender, contact e-mail address, physical address, telephone numbers, screen names, websites, and other person identifiers
    - All activity logs showing all user posts and other Facebook activities
    - All electronic mail
    - Images
    - GPS tags
    - Text messages
    - Comments
    - Likes
    - Histories
    - Buddy lists
    - *Individuals following and individuals followed*
    - Profiles
    - Method of payment
    - *Detailed billing records*
    - Access logs
    - Transactional data
    - All Photoprints, including all photos uploaded by the user and all photos uploaded by any user that has the subject user “tagged”, including EXIF data
    - All Neoprints, including profile contact information; *news feed information; status updates; links to videos, photographs, articles and other items*; Notes, Wall postings; friend lists, including the friends’ Facebook user identification number; *groups and networks of which the user is a member*, including the groups’ Facebook group identification numbers; *future and past event postings*; rejected “Friend” requests; comments; gifts; pokes; tags; and *information about the user’s access and use of Facebook applications*
    - All other records of communications and messages made or received by the user, including *all private messages, chat history, video calling history*, and *pending “Friend” requests*.

According to the warrant application the seizure of all of this information was justified because California Highway Patrol Investigator Jenna Jones looked at Mr. X’s Facebook profile and “viewed photos of X with women having Russian names. One of the photos. . . has X standing next to a woman who I recognize from the Backpage subpoena return . . . Currently, this woman has not been identified by law enforcement.” *See* Ex. B at 13.

Again the government promises that the information received from Facebook will be searched according to “Procedures for Electronically Stored Information. Ex. B, Attachment B, Page 27. Again, there are no actual “Procedures” described, but merely language explaining that searching the Facebook account is complicated and time-consuming. Ex. B, Affidavit, Page 23-24.

Results of this warrant are pending.

# The Dell Inspiron warrant request to search entire computer

The magistrate issued a warrant to search the entire contents of Mr. X’s personal computer, a Dell Inspiron 15. *See* Ex. C, Dell Inspiron Warrant at page 18, paragraph d. (requesting permission to create a forensic image (“A forensic image is an exact physical copy of the hard drive or other media.”))

The Dell Inspiron was supposed to be searched according to “Procedures for Electronically Stored Information. Ex. C, Attachment B, Page 25. Yet again, no actual procedures for conducting a search of the laptop were provided or described. Ex. C, Affidavit, Page 16-22. Rather than provide a procedure for searching for relevant data, the application explains that forensic analysis is expected to be difficult and time consuming. Ex. C. 18-22. It goes on to state “seizure pursuant to this warrant may require a range of data analysis techniques, including hashtag tools to identify evidence subject to seizure pursuant to this warrant, and *to exclude certain data from analysis, such as known operating system and application files*.” Ex. C at 22.

The discovery from the Dell account provided to Mr. X’s counsel make evident that Mr. X’s entire computer was searched including the following:

* Image of The City of Miami, Florida city stamp;
* Images from Game of Thrones
* Mr. X’s web browser history

# The warrant to search the entirety of five electronic devices

The magistrate issued a warrant through the entire contents of Mr. X’s five electronic devices. *See* Ex. D, Affidavit at page 29, paragraph d. (requesting permission to create a forensic image (“A forensic image is an exact physical copy of the hard drive or other media.”)) One generic boilerplate warrant was used to search five very different electronic devices. CHP Investigator Jones offered no particularized evidence or reasoning why there was probable cause to search the devices. Rather, the following generic reasoning was provided:

Individuals involved in illicit commercial sex use cellular telephones, tablets, desktops and notebook computers and maintain these items on their person and/or in their residences and/or business fronts. Individuals involved in illicit commercial sex use cellular telephones, tablets and notebook computers to increase their mobility, coordinate illicit activities, and to provide pimps and prostitutes with instant access to phone calls, voice messages, text messages, instant messaging

(IM) and internet based correspondence. These electronic devices allow individuals involved in illicit commercial sex to maintain contact with other pimps, prostitutes, complicit businesses, and clients. These electronic devices contain wire and electronic data concerning telephonic contact records, text messages, and electronic mail messages with co-conspirators and clients, as well as telephone books containing contact information for co-conspirators and clients. Individuals involved in illicit commercial sex also utilize digital cameras, cellular telephones, tablets, desktop and notebook computers with photograph and video capabilities to take photographs and videos of themselves as well as other co-conspirators for the purpose of electronic advertising and promotion of prostitution. Moreover, I know that digital evidence can be stored on a variety of systems and storage devices including hard drives, SDs, DVDs, Ipads, Ipods, thumb drives, flasj drives, and portable hard drives.

Ex. D at 18.

The search warrant affidavit purports to set forth the procedures and methodology agents will use when searching the seized electronic devices. See Exh. D, pp. 19-20; 23-27. For instance, the “Cell Phone Methodology” portion indicates, in relevant part: “identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review….” Exh. D, p. 20. In other words, the agents have unbridled discretion to parse all contents of the phone.

The same methods are applied to other forms of media. After explaining how difficult it is to analyze digital media, the affidavit explains: “identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques….” *Id*. at 26. The problem is that the phrase “a range of data analysis techniques” has no special industry meaning. That could just mean that the agents are going to turn on the devices, and start clicking on folders. Such procedures are neither a legal methodology nor reasonable. That is to say that no search protocols were described.

Ultimately, the government imaged and searched the entirety of the five devices. What they found was a mind-boggling amount of information:

* Apple iPad
  + 301 calls in call log
  + 139 contacts
  + 75 cookies
  + 26 webpages in web history (including Comedy Club website)
  + 5,214 images (including countless pictures of food)
  + and many other kinds of data and information
* Samsung Galaxy
  + 156 Device locations (providing GPS coordinates for phone 156 times with time stamp)
  + 32 audio files
  + 17 documents
  + 2,214 images
  + 58 videos
  + and many other kinds of data and information
* BLU Star JR
  + 33 MMS messages
  + 9597 SMS messages
  + 205 contacts
  + 500 calls in call log
  + and many other kinds of data and information
* Nokia
  + 300 calls in call log
  + 43 contacts
  + 365 SMS Messages
  + 328 Datat Files for applications
  + 3330 music files
  + 8,193 images (including photos of pandas and legos)
  + 3 videos
  + and many other kinds of data and information
* HTC Cell phone
  + 4224 text messages
  + 227 contacts
  + 300 phone calls in call log
    - 146 Incoming
    - 27 Missed
    - 127 Outgoing
  + 36 images (for example a sand castle at the Del Coronado Hotel)
  + 1 video (of an identifiable person driving a car)
  + and many other kinds of data and information

After reviewing the contents of these searches, there is very little that the government does not know about Mr. X’s life. This was not the reason for the search. It was not the search that was authorized. The fruits should be suppressed.

# III. ARGUMENT

**The Court should suppress the fruits of the four overbroad warrants that lacked probable cause and particularized suspicion for the various categories of information obtained from each account and device.**

## *Summary of Argument*

The warrant for, and subsequent search of, Mr. X’s Google, Facebook, and six electronic devices violated his Fourth Amendment rights in the following ways:

* First, there was insufficient probable cause to establish that evidence of criminal sex acts would be present on Mr. X’s account.
* Second, the warrant was overbroad in violation of the Fourth Amendment’s particularity requirement.

Moreover, the government should have provided the court with methods and procedures it would use to look in limited areas of the computer for limited information. Instead, as a result of the overbroad and unsupported search warrants, the government seized over thousands upon thousands of pages of information. For the reasons that follow, this Court should suppress all evidence seized in connection with the search and seizure of the Google account, Facebook account, and six electronic devices.

## *Mr. X has a reasonable expectation of privacy in the electronic information and devices* seized.

* 1. The Google accounts

Google is an internet based search engine and webmail provider. Users may set up an account allowing them to send and receive electronic mail, store contacts, instant mail, video chat and create documents which can be edited by multiple people (the google docs feature). Additionally, when a person’s gmail account is open, Google monitors the internet searches and websites visited by the user.

Electronic mail is subject to the same Fourth Amendment protections as traditional mail because individuals maintain a reasonable expectation of privacy in these communications. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (“Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”); *United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) (Reasonable expectation of privacy recognized for “private information, including emails” stored on a cellular phone.); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (“The privacy interests in these two forms of communication [email and traditional mail] are identical.”).

* 1. The Facebook account

Facebook is an online social media tool akin to a digital diary, in which a user creates a ‘profile,’ consisting of photographs, personal information (school and work history, political beliefs, birthday, gender etc…). Users may request to become ‘friends’ with one another, thus allowing reciprocal access to each other’s Facebook profile. Users can post ‘status updates’ (something like a short diary entry), photographs, news articles, etc… which will be viewed by their ‘friends’ in their ‘newsfeed.’

The ‘newsfeed’ is a sequential list of posts by a user’s ‘friends.’ A user can ‘like’ or ‘comment’ on their ‘friends’ posts. A user can also post directly on a ‘friend’s’ ‘wall,’ thus contributing to her ‘friend’s’ digital diary. Facebook also provides the ability to communicate privately with other users, in a manner similar to email:

Here it is important to note that Facebook provides different means of communication. Postings to a user’s “wall” are generally accessible by the user’s Facebook “friends,” a potentially large group of acquaintances. Other sorts of messages operate in the same manner as email—that is, they are sent from one user to one or more specified users. They are not open to public perusal by one’s “friends” or by the general public.

*R.S. v. Minnewaska Area School District No. 2149*, 894 F. Supp.2d 1128 (D. Minnesota, September 6, 2012). At least one district court has held that private Facebook messages are subject to the same Fourth Amendment protections as email. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp.2d 965, 991 (C.D. Cal. 2010).

* 1. The Dell Inspiron laptop and the five digital devices

The Ninth Circuit has expressly recognized the constitutionally protected privacy interest in one’s digital devices:

Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their “papers.”

*United States v. Cotterman*, 709 F.3d 952, 964 (9th 2013). In holding that digital devices are the modern equivalent of “papers” for Fourth Amendment purposes, the Court acknowledged that privacy concern at stake implicates the “safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government.” *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, C.J., dissenting); *see also New York v. P.J. Video, Inc.,* 475 U.S. 868, 873, 106 S.Ct. 1610, 89 L.Ed.2d 871 (1986).

All of the records sought and searched by the government pursuant to the warrants are expected to remain private and these expectations are “one[s] that society is prepared to recognize as ‘reasonable.’ ” *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring).

# The warrants in this case were not based on probable cause

“[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend IV. The probable cause requirement is intended to protect “citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime.” *Brinegar v. United States*, 338 U.S. 160, 176 (1949). It has been defined as “where known facts and circumstances warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found.” *Ornelas v. United States*, 517 U.S. 690, 696 (1996). Reasonable suspicion, a lower standard, requires particularized and objective facts giving rise to suspicion that criminal activity is afoot. *See Michigan v. Long*, 463 U.S. 1032 (1983).

There was not probable cause to search the entirety of Mr. X’s accounts and electronic devices.

* 1. *The Google account warrant lacked probable cause for the breadth of materials requested.*

The government had reason to believe that the [thisisprivate@gmail.com](mailto:thisisprivate@gmail.com) account was used to book a hotel room that was used for criminal sex acts in December 2014 because of the statements of one of the complaining witnesses and hotel staff. Rather than requesting information from Google about emails pertaining to hotels during this month. The government sought and received a warrant for the entirety of the account information from July1, 2014 to January 26, 2015. There was not probable cause to seize and search all of this information and for this long of a time period.

The government had reason to believe that the [dontlookhere@gmail.com](mailto:dontlookhere@gmail.com) and [noneofyourbusiness@gmail.com](mailto:noneofyourbusiness@gmail.com) accounts were used to post Backpage.com ads in December 2014. Rather than requesting information from Google about emails pertaining Backpage.com during this month, the government sought and obtained a warrant for the entirety of the accounts information from July 1, 2014 to January 26, 2015. There was not probable cause to seize and search all of this information and for this long of a time period.

* 1. *There was no probable cause to search the Facebook account.*

The government states there was one photograph on Facebook linking Mr. X with a woman who appeared in a Backpage.com ad. The Backpage.com ad was posted on August 3, 2014 and listed a phone number associated with Mr. X. The woman in the photograph had not been identified by the government, and is not the subject of the charges in this case. There is nothing apparently illegal about a Backpage.com ad. Indeed, there is no evidence that Facebook was used to accomplish any of the criminal acts alleged in this case. Thus, there was no probable cause to issue a warrant to search the Facebook account.

Even if the Court disagrees and finds that there was probable cause, the government did not seek a more limited request to seize and search information regarding the woman’s identity. Instead, the government sought and received a warrant for the entirety of the account information from July1, 2014 to January 2015. There was not probable cause to seize and search the breadth of information listed in the warrant.

* 1. *There was no probable cause to search the Dell Inspiron*

There was no probable cause to search the computer at all and certainly not the entire computer. The computer was seized from the hotel room of one of the complaining witnesses (“V2”) at the Western Inn hotel room #379. Nothing in the warrant request stated that this particular electronic device had been used to further any criminal sex acts. The only connection to any of the criminal sex acts was that it was in the same room as one of the complaining witnesses. Thus, there was no nexus connecting the Dell Inspiron to the criminal sex acts in the warrant. Even if there was a minimal nexus, that nexus did not provide grounds to rummage through the entirety of the device. The government should have provided the court methods and procedures it would use to look in limited areas of the computer for limited information.

* 1. *There was no probable cause to search the other five electronic devices*

There was no probable to search the electronic devices at all and certainly not each and every one of them in their entirety. The computer was seized from Mr. X’s vehicle when he was arrested. Nothing in the warrant application stated that these particular electronic device had been used to further any criminal sex acts. The only connection to any of the criminal sex acts was that it was seized from Mr. X’s vehicle. Thus, there was no nexus connecting the five electronic devices to the criminal sex acts. Even if there was a minimal nexus, that nexus did not provide grounds to rummage through the entirety of the devices. The government should have provided the court methods and procedures it would use to look in limited areas of the devices and stated what limited information they were searching for.

# Probable cause to search email, social media accounts, and electronic devices for one type of “file” or communication cannot justify searching the entire account.

* 1. *The particularity requirement is especially important in cases involving email, social media and electronic devices*.

The Fourth Amendment requires a warrant to be limited in scope to prevent the “general, exploratory rummaging in a person's belongings.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). This concept is referred to as breadth and “may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant.” *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 57 (9th Cir.1991). “[P]robable cause means a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of circumstances.” *United States v. Diaz*, 491 F.3d 1074, 1078 (9th Cir. 2007) (internal quotation marks omitted). Particularity is a lynchpin of the Fourth Amendment analysis, defining the breadth of a permissible search:

[T]he scope of a lawful search is ‘defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawn-mower may be found in a garage will not support a warrant to search the upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.

*Maryland v. Garrison*, 480 U.S. 79, 85-85 (1987) citing *United States v. Ross*, 456 U.S. 798 (1982). These types of physical limitations are absent in the digital world “where size or other outwardly visible characteristics of a file may disclose nothing about its content.” *United States v. Galpin*, 720 F.3d. 436, 447 (2d. Cir. 2013). Thus, a warrant may not be so broad as to encompass nearly everything in a location to be searched, effectively obviating the particularity requirement, and amounting to the general warrant dreaded by the Constitution's Framers. *See Marron v. United States*, 275 U.S. 192, 196 (1927).

The Ninth Circuit addressed the issue of over-breadth in *United States v. Bridges*, 344 F.3d 1010 (9th Cir. 2003). There, the court noted that "[s]earch warrants . . . are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet of personal papers and property to be seized at the discretion of the state." *Id.* at 1017. The court noted that the warrant's list of items to be seized was:

so expansive that its language authorize[d] the government to seize almost all of the [business's] property, papers, and office equipment in Billings. The list is a comprehensive laundry list of sundry goods and inventory that one would readily expect to discover in any small or medium-sized business in the United States.

*Id.* The court went on to note that the warrant "delineated no clear material *limitation* or boundary as to its scope." *Id.*

In another recent case, the Ninth Circuit explained:

The reality that over-seizing is an inherent part of the electronic search process requires this Court to exercise greater vigilance in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect.

*United States v. Schesso*, 730 F3d 1040, 1042 (9th Cir. 2013) (citing *United States v. Comprehensive Drug Testing Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010).

The principal of particularity takes on a special role in protecting privacy when the police seize and search a social media account. The right to be free from general warrants developed when no information was stored digitally, and thus all recorded private information took up tangible space. Social Media accounts, however, can contain abundant information that is accessed and stored at many locations throughout the physical world.

These facts of modern, digital life led to the unanimous decision in *Riley*, where the Supreme Court held that police officers may not search a smartphone based on probable cause to arrest its owner. Instead they must “get a warrant.” 134 S. Ct. 2473, 2495 (2014).

The Supreme Court’s reasoning in *Riley* has clear implications for the kind of warrant that officers must get. The Court recognized that the volume, variety, and sensitivity of the information stored in the smartphone or stored remotely (in “the cloud”) and accessed through the smartphone led the Court to conclude that the privacy interests involved in smartphone searches “dwarf” those examined in past cases, when only limited information contained in a finite space was involved. *Id*. at 2491.

Applying this reasoning, a federal district court in Illinois held that a warrant to search all content on a device is invalid when the police fail to demonstrate probable cause that everything on the phone is evidence. *United States v. Winn*, U.S. Dist. Ct., No. 14CR30169-NJR slip op. at 10 (S.D. Ill. Feb 9, 2015), *appeal filed*, No. 15-1500 (7th Cir. March 9, 2015). In that case, witnesses alleged that the defendant had been pointing his smartphone in the direction of young girls at a swimming pool and either photographing or videotaping them. But, as in this case, the police did not tailor a warrant request to the types of files as to which they had probable cause. Instead, they copied a template seeking authorization for the broadest search possible, a search encompassing an expansive range of data.

The district court held that this approach violated the Fourth Amendment because it ran afoul of the particularity requirement. The court reasoned that, because the officer obtained the warrant based on accusations about Winn’s behavior at the swimming pool, the officers had probable cause only to investigate the crime of public indecency. But “only two categories of data could possibly be evidence of [that crime]: photos and videos.” *Id*. at 9. Indeed, “the narrative portion of the complaint did not even mention [other] categories of data.” *Id*. Thus, officers could not permissibly rely on a template that failed to differentiate one category from another:

Templates are, of course, fine to use as a starting point. But they must be tailored to the facts of each case. This particular template authorized the seizure of virtually every piece of data that could conceivably be found on the phone Obviously,

the police will not have probable cause to search through and seize such an expansive array of data every time they search a cell phone.

*Id*., citing *Riley*, 134 S. Ct. at 2491.

As to the files for which no probable cause existed, the court ruled that the police should have established probable cause as to each type of data. Their failure to do so at the time they applied for the warrant was fatal to its validity:

The bottom line is that is Detective Lambert wanted to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to Winn’s criminal activity, and he did not do so. Consequently, the warrant was overbroad, because it allowed the police to search for and seize broad swaths of data without probable cause to believe it constituted evidence.

*Id*. at 10.

* 1. *The warrants in this case were not sufficiently particularized***.**

The particularity required of warrants to search social media accounts and electronic devices was not on display here. The police failed to present facts to the magistrate supplying particularized probable cause about what particular information from Mr. X’s Google accounts, Facebook account, Dell Inspiron laptop and five digital devices would yield evidence of a crime. Rather, the warrants sought permission to search the entirety of the accounts over an overbroad period of time and the entirety of the six devices. Accordingly, the warrants relied upon to search were invalid.

* 1. *Suppressing All Evidence From the Search Is the Appropriate Remedy*

The remedy for an overbroad search warrant is suppression of the seized evidence. *United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994); *see also United States v. Stubbs*, 873 F.2d 210 (9th Cir. 1989). Because the search warrant is so overbroad, the government cannot rely on the *Leon* exception. *See United States v. Michaelian*, 803 F.2d 1042, 1046 (9th Cir.1986) (a warrant may be “so facially overbroad as to preclude reasonable reliance by the executing officers.”). Therefore, the evidence seized and derived from the search warrant should be suppressed. *See Wong Sun v. United States*, 371 U.S. 471.