Obtaining and Using Electronic Evidence and Social Media

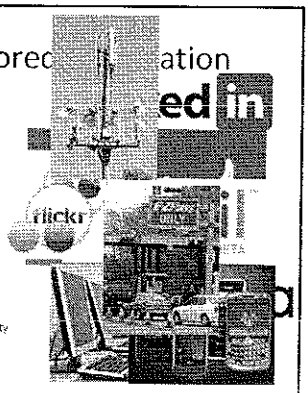
Adam Candeub
Michigan State University College of Law
Michigan State Appellate Defender Office and Criminal Defense Resource Center
October 19, 2013

Today's Talk

- What's Electronically Stored Information (ESI)?
  - Varieties
  - Who has it
- How to get it?
  - Civil context: Rule 26
  - Criminal
    - Government: Stored Communications Act
    - Defendant: Rule 16, 17
- How to get it in?
  - Authentication
  - Hearsay Issues

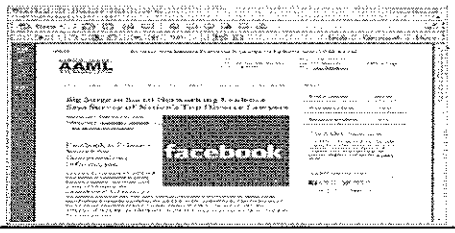
Electronic Storec ation

- Data in your computers
  - Laptops, desktops, etc.
  - Cell phones
  - Tablets
- Data in others' computers
  - Electronic toll records
  - ATM withdrawals
  - Smart energy records
  - Surveillance camera
- Personal Use Cloud Data Storage
  - Facebook/MySpace/LinkedIn
  - Email
  - Flickr
  - Chat boards, forums, Wikipedia
- Records of communications, internet activity
  - ISP IP address logs
  - Cell phone location records



Social Media

- It's our lives
- 81% of the attorneys reported finding and using evidence from social networking sites



Public Social Media

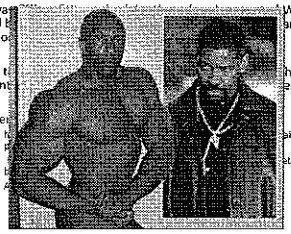
- Much social media is public
  - Spokeo.com
  - Facebook public profiles
- What about befriending witnesses, parties?
  - Ethical concerns: Rules of Professional Conduct
    - Rule 4.2 : lawyer may not communicate, or cause another person to communicate, with a person represented by counsel
    - Rule 4.1: lawyer may not "make a false statement of material fact or law to a third person" in course of representation
  - See N.Y. City Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2010-2 (2010), http:// www.nycbar.org/pdf/report/uploads/20071997-FormalOpinion2010-2.pdf.

Public info is revealing in many ways

- Most lawyers think photos, videos, and statements posted on a social networking site are made public
  - Many people really don't understand Facebook privacy settings
- But also . . . Stuff that is typically *not* private
  - Emoticons
    - In personal-injury cases, the "smiley face" used by a plaintiff claiming to be in serious pain or severely depressed can be used against them
  - Friends lists

Facebook: It's not just incriminating pictures and photos

- In a New York case involving allegations of police brutality, Vaughan Waters, who was on parole after being convicted of burglary, and was charge of carrying a loaded weapon.
- It wa… Waters in 2006, the accused had t… an extra 15-bullet magazine, 27 lo…
- But t… had been planted on his client… est.
- Defe…
  - …ining Day "to brush up on proper …
  - …te with an angry red emoticon
  - …



Facebook: Log Info

- 19 year-o… …oklyn, New York was … …h a robbery
- But Bradford was on Facebook at the time, updating his status to read

  "on the phone with this fat chick . . . wherer my i hop [sic]"

OTOH Bishop v. Minichiello, 2009 BCSC 358 (Can.).

- Bishop claimed that he was physically unable to return to his job, which involved office work at a computer.
- But court allowed plaintiff's Facebook log-on/log-off server records to demonstrate his extensive late-night computer usage

People v. Liceaga, 2009 Mich. App. LEXIS 160 (Mich. Ct. App. Jan. 27, 2009)

- In murder case, the prosecutor sought to admit photos from the defendant's MySpace page (which showed the defendant holding the gun allegedly used in the crime, and in which he was displaying a gang sign) as evidence of intent and planning.
- Michigan Rule of Evidence 404(b)(1) allows evidence for the limited purpose of proving intent and showing a characteristic plan or scheme in committing the offense
- The appellate court upheld the admission, finding that its probative value exceeded any danger of unfair prejudice.

Ohio v Gaskins, No. No. 06CA0086-M, 2007 __ Ohio __ 4103, (Ct. of Appeals Ninth Judicial District)

- In a statutory rape case, court permitted defendant to introduce evidence that the victim had held herself as on her MySpace page as an 18 year-old.
- Photos of the girl that she had posted were admitted, along with witness testimony about their authenticity.
- But, court upheld exclusion of questioning about pictures when no evidence that Def. ever saw them

PRISM and Government Surveillance as a Shield

- United States of America v. Daryl Davis, Hasam Williams, et al., Case No. 11-60285-cr-rosenbaum (U.S. Dist. S. Florida)
- Defendant alleges exculpatory cell phone metadata
  - Data lost by cellphone company
- Defendant subpoena NSA and PRISM program
  - Fed. R. Crim. P. 16(a)(1)(E) quite broad

(E) *Documents and Objects*. Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

(i) the item is material to preparing the defense;

(ii) the government intends to use the item in its case-in-chief at trial; or

(iii) the item was obtained from or belongs to the defendant.

Court interprets motion as a motion pursuant to FISA, 50 U.S.C. Section 1806

(f) In camera and ex parte review by district court

. . . whenever any motion or request is made by an aggrieved person pursuant to . . . . obtain applications or orders or other materials relating to electronic surveillance . . . the United States district court . . . Shall . . . if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Government argues CIPA applies

- The Classified Information Procedures Act ("CIPA"), 18 App. U.S.C., Section 4
- "The court may permit the United States to make a request for [relief from discovery] in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal."
- *The end of the adversarial system?*

Cell phones & Search Incident to Arrest

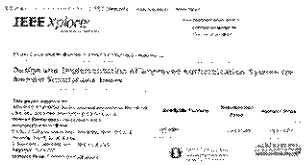
- Atwater v. Lago Vista, 532 U.S. 318 (2001)
  - Police may arrest for trivial, misdemeanor offenses
- Chimel v. California, 395 U. S. 752 (1969)
  - Police may search incident to arrest only the space within an arrestee's " 'immediate control'"

Smartphones

- Smartphone is just like any other container
  - Police may search incident to arrest (for 5-10 minutes)
  - *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007)
- *No, smartphones are different*
  - *State v. Smith*, 920 N.E.2d 949 (Ohio 2009)

Weird ca

- If s
  20
  cra
  thi



- Th

How to get it? Depends on who you are.

- In civil context, subpoena, issue discovery against legal custodian of the ESI
  - E.g., Facebook account holder
  - Stored Communications Act blocks individuals from subpoena-ing Facebook
- In criminal context,
  - If you're the government, Stored Communications Act helps you out, as it requires Facebook to provide info.
  - If you're the defendant, you must rely on Rules 16, 17 of criminal procedure
  - Other methods . . . .
    - Public Facebook pages

Civil Suits

- In complex civil litigation, the number of documents is staggering
- It's not your Dad's discovery anymore

General Rule: Social Media Discoverable in Civil Litigation

- Social media and other ESI OK
  - "if the discovery appears reasonably calculated to lead to the discovery of admissible evidence"
  - Facebook postings not privileged and their disclosure does nt infringe upon a right of privacy.
  - Disclosure OK under the traditional discovery principles of Fed.R.Civ.P. 26(b), that is, "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense"
- Tompkins v. Detroit Metropolitan Airport, 278 F.R.D. 387 (E.D.Mich.,2012)

In civil suits, control threshold for production low

- Flagg v. City of Detroit, No. 05-74253, 2008 WL 787061, at *1 (E.D. Mich. March 20, 2008)
  - city *(not* ISP*)* was compelled to produce the text messages of former Mayor Kwame Kilpatrick and the employee with whom he was having an affair
  - records held by an Internet service provider were within the city's constructive control and custody

Privacy Arguments Typically Fail

- School Board subpoenaed plaintiff's social media in sexual harassment case; court said no on privacy grounds
  - See T.V. v. Union Twp. Bd. of Educ. No. UNN-L-4479-04, 2007. LEXIS 3005 (N.J. Super. Ct. Law. Div. June 8, 2007)
- (Much) more common view
  - Bass ex rel. Bass v. Miss Porter's Sch., 738 F. Supp. 2d 307, 323 (D. Conn. 2010) (no privacy)

Barnes v. CUS Nashville, 2010 WL 2265668 (M.D. Tenn. June 3, 2010)

- One solution to privacy
- Slip and fall while dancing on a bar at the "Coyote Ugly Saloon" in Nashville
- Magistrate Judge offered to create his own Facebook account and "friend" the plaintiff for the sole purpose of reviewing, *in camera,* photos she had posted on Facebook of herself dancing on the bar on the night of incident

SCA and ESI

- In civil context, ESI received from parties own hands, *not* the ISP, social media site, etc.
- Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) prevents parties from going directly to "electronic storage providers" and "remote computing services"
- SCA interpreted to include ISPs, YouTube, Facebook, Gmail, restricted electronic bulletin boards

Government, ESI, and SCA

- SCA forbids ISPs, websites, etc. from giving information to private person under most circumstances
- SCA gives government broad power to obtain information
  - Contents of emails (180 days or younger) with warrant
  - Contents of emails (over 180 days) with simply a section 2703(d) order which merely requires a showing of relevance to criminal inquiry

Non-content records and section 2703(d) orders

- Information includes
  - The email addresses of those customer sends and receives email---and the size of the email
  - The IP addresses of other computers on the Internet that customers communicate with, when, and how much data exchanged
  - The web addresses of the web pages that you visit,
  - *cell phone locations*
- Government can obtain in several ways.
  - Warrant
  - 2703(d) order which issues upon "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation "

Basic Subscriber info

- Subpoena generally enough
- This info includes
  - Name
  - Address
  - Service start dates and the types of services you use.
  - Sign on and off times, the length of each session, and the IP address that the ISP assigned to you for each session
  - How bills are paid and any credit card or bank account number the ISP or phone company has on file
- Thus, PRISM is born . . . .

Issue for future: Status of geolocation data

- Currently, most cell tower data (in most jurisdictions) can be obtained with a section 2703(d) orders
  - Some jurisdictions require warrant, some subpoena

- Some geolocation data requires nothing

- Will United State v. Jones change anything?

IN RE: APPLICATION OF THE UNITED STATES OF AMERICA FOR HISTORICAL CELL SITE DATA. No. 11-20884 (5th Cir. July 31, 2013)

- No expectation of privacy in historical cellphone data
- Warrant not required . . . .

Civil versus criminal e-discovery

- FRCP explicit treatment of ESI and mandatory methods of treatment, i.e., Rule 26 meet and confer meetings, Rule 16 scheduling orders
- E-discovery is a mess in the criminal context in complicated white collar cases involving lots of documents

Rules of Criminal Procedure

- Rule 16 (for evidence in the custody of the government) or Rule 17 (for evidence in the possession of third parties)
- But no equivalent rules for sharing data, shifting costs, clawbacks, etc. found in civil litigation
- Instead added complications, added complications of the 4th and 6th Amendment, Jenks Act, Brady Act

How to get ESI in?

- Relevance
- Authentication
- Hearsay

Authentication: 2 main issues

- Identity of the alleged declarant
  - Identity often denied
  - E.g., Connecticut v. Eleck, 23 A.3d 818, 820 (Conn. App. Ct. 2011) (someone else got into account)
- Proffered evidence of the alleged communication is an accurate representation of what was really posted online.
  - Fairly easy to do
    - United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (finding officer's testimony that the chat room printout "fairly and fully reproduced the chats between her and [the defendant]" was sufficient to authenticate)
    - United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (finding that the chat room log printouts were authenticated based on a co-conspirator's testimony that printouts appeared to be an accurate representation of the chat room conversations among the conspirators).

How to do it? Authentication for online materials

- Testimony of a witness with personal knowledge of the document (Rule 901(b)(1))
- If no personal testimony, a witness who has general personal knowledge of how that type of exhibit is routinely made can authenticate or comparison with authenticated example
  - Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007); 901(b)(3)
- Distinctive characteristics of the communication, including circumstances 901(b)(4)
- Trade inscriptions (902(11)), Public records (901(b)(7), System or process capable of proving a reliable result (901(b)(9), Official publication (902(5))
- Rule 902, FRE, identifies 12 methods by which electronic evidence may be self-authenticated, meaning that extrinsic evidence is not necessary for admissibility. Although some forms of electronic evidence can be self-authenticating (e.g., government websites), most forms of Internet-based communications are not self-authenticating.

Individualization, "Distinctive Characteristics," and Authentication

- Quite often, courts look to the degree of individualization that social networking profiles for authentication and admissibility.
- In Griffin v. State, 995 A.2d 791, 806 (Md. Ct. Spec. App. 2010), a murder case, the printout was a redacted page from a MySpace profile belonging to the appellant's girlfriend, who had allegedly threatened an eyewitness via MySpace by writing, "JUST REMEMBER, SNITCHES GET STITCHES!! U KNOW WHO YOU [ARE]!!"
- Printout in question came from a profile bearing the girlfriend's user name of "Sista Souljah," listing her birth date, featuring a photo of her and the appellant embracing, and including a blurb of the appellant's nickname "FREE BOOZY."
- The court held that such individualization was more than enough to authenticate that the MySpace profile was hers.

Email, Text Messages, Tweets

- When dealing with e-mails or personal messages directly sent between users, "a recipient, or non-recipient with knowledge that the communication was sent, may authenticate."
  - United States v. Safavian, 435 F. Supp. 2d 36, 40 n.2 (D.D.C. 2006); (Shea v. Texas, 167 S.W.3d 98, 105 (Tex. Crim. App. 2005)
- witness who has general personal knowledge of how that type of exhibit is routinely made can authenticate or comparison with authenticated example
- Trade inscriptions
- Certified copies of business records

Computer Stored Records and Data

- Testimony of a witness with personal knowledge of the document
- Witness who has general personal knowledge of how that type of exhibit is routinely made can authenticate or comparison with authenticated example
- Distinctive Characteristics
- System or procdess capable of proving a reliable result

Website Postings and Blogs

- Testimony from the webmaster, or even simply an individual who viewed that site and can verify the accuracy of the offered evidence
  In re Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004)
- If no personal testimony, a witness who has general personal knowledge of how that type of exhibit is routinely made can authenticate or comparison with authenticated example
  - Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007); 901(b)(3)
- Public records (901(b)(7), System or procdess capable of proving a reliable result (901(b)(9), Official publication (902(5))

Low evidentiary bar:
Ohio v. Bell, 882 N.E .2d 502, 511 (Ohio Ct. App. 2009)

- Court affirmed the trial court's denial of a defense motion to exclude printouts of MySpace instant messages alleged to have been sent to a victim by the defendant under his MySpace screen name.
- Noting that the evidence required to meet the authentication threshold for admissibility is low, the court was not persuaded by defense arguments that MySpace chats can be readily edited after the fact from a user's homepage.

Authentication: In the Interest of: F.P 878 A.2d 91 (Pa. Super. 2005)

- Instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404."
- Z.G. testified
  - his screen name is WHITEBOY Z. Z.G.
  - printed the instant messages off his computer.
  - believed the Icp4Life30 in the conversation to be appellant.
- Court approved admission
  - "e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa.R.E. 901 and Pennsylvania case law."
  - Authenticaltion is satisfied
    - by evidence sufficient to support a finding that the matter in question is what its proponent claims." Pa.R.E. 901(a). T
    - testimony of a witness with personal knowledge that a matter is what it is claimed to be may be sufficient to authenticate or identify the evidence.
    - *Commonwealth v. Brooks*, 352 Pa.Super. 394, 508 A.2d 316, 318 (1986) ("The courts of this Commonwealth have demonstrated the wide variety of types of circumstantial evidence that will enable a proponent to authenticate a writing.")

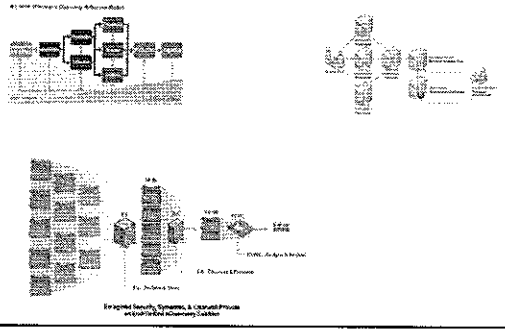
Hearsay: Email

- Generally same as those associated with conventional correspondence. *Hood-O'Hara v. Wills*, 873 A.2d 757, 760 (Pa. Super. 2005).
- Several exceptions often tried
  - *Business Record Exception: Usually fails because email not regularly produced*
    - *Rambus, Inc. v. Infineon Techs. AG*, 348 F. Supp. 2d 698, 707 (E.D. Va. 2004) ("Email is far less of a systematic business activity than a monthly inventory printout")
  - Present sense
  - Party opponent admissions

Often emails and posting admitted not for truth of contents

- Email/ internet postings can be offered to establish other persons had accessed and viewed web-page and to show that technology was known and used prior to certain date
  - *CA, Inc. v. Simple.com, Inc.*, 780 F.Supp.2d 196 (E.D. N.Y. 2009)

E-discovery in the civil vs. criminal context



In conclusion . . . .

- True e-discovery could transform criminal justice system . . . . But there needs to be political will and vision