Mobile Devices & Privacy

Regulations, Laws, Cases, and Technical Measures Which Affect First Amendment Rights

July 2012

Prepared by: **Kevin W. Wimberly**

Overview

- Mobile Apps Update since Winter 2012 Meeting
  - FTC – increased interest in mobile apps
  - Privacy Policies
  - California – iOS litigation
- F*&# tha Police (Film the Police)
  - Mobile Spring
  - Apps
  - Eavesdropping Statutes
  - Recent Cases
- Security Issues
  - Compelled password divulgence and encryption

- FTC Report Raises Privacy Questions About Mobile Applications for Children
  - "Mobile Apps for Kids: Current Privacy Disclosures Are Dis***app***ointing" (emphasis [sadly] in original)
- Paper, Plastic . . . or Mobile? An FTC Workshop on Mobile Payments

California: We Got the FTC's Back

- February 22, 2012 - Attorney General's Agreement with Amazon, Apple, Google, Hewlett-Packard, Microsoft, and RIM:
  - From the Press Release: "This agreement will allow consumers the opportunity to review an app's privacy policy before they download the app rather than after, and will offer consumers a consistent location for an app's privacy policy on the application-download screen. If developers do not comply with their stated privacy policies, they can be prosecuted under California's Unfair Competition Law and/or False Advertising Law."
- Facebook joined in June 2012.

California: We Got the FTC's Back

- Mobile Apps Market Companies will include, in the application submission process for new or updated apps, either (a) an optional data field for **a hyperlink to the app's privacy policy or a statement describing the app's privacy practices** or (b) an optional data field for the **text of the app's privacy policy or a statement describing the app's privacy practices**. For developers who choose to submit a hyperlink or text in the available data field, the Mobile Apps Market Companies will enable access to the hyperlink or text from the mobile application store

- The Mobile Apps Market Companies have, or will implement a **means for users to report** to the Mobile Platform Companies apps that do not comply with applicable terms of service and/or laws.

- The Mobile Apps Market Companies have or will implement a **process for responding to reported instances of non-compliance with applicable terms of service and/or laws**. Any action that a Mobile Apps Market Company takes with respect to such an application will not limit law enforcement or any other regulator's right to pursue an action against a developer for alleged violation of applicable law.

California: iOS Litigation

- *In re iPhone Application Litigation* (N.D. Cal. June 12, 2012)
  - Class action
  - Apple represented that it takes administrative, technical, and physical measures to "safeguard your information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction."
  - Plaintiffs allege that Apple (and other Defendants) violated their privacy rights by allowing third party apps to collect and make commercial use of personal information without the users' consent or knowledge.
    - Geolocation data, e-mail addresses, home/work locations, gender, age, passwords, etc.

California: iOS Litigation

- *In re iPhone Application Litigation* (N.D. Cal. June 12, 2012)
- Claims vs. Apple:
  - Stored Communications Act
  - Wiretap Act
  - Invasion of Privacy (Cal. Const.)
  - Negligence
  - Computer Fraud and Abuse Act
  - Trespass
  - Conversion
  - Consumer Legal Remedies Act (Cal.)
  - Unfair Competition (Cal. Bus. & Profs. Code § 17200)

California: iOS Litigation

- *In re iPhone Application Litigation* (N.D. Cal. June 12, 2012)
- Claims vs. Apple:
  - Stored Communications Act - DISMISSED
  - Wiretap Act - DISMISSED
  - Invasion of Privacy (Cal. Const.) - DISMISSED
  - Negligence - DISMISSED
  - Computer Fraud and Abuse Act - DISMISSED
  - Trespass - DISMISSED
  - Conversion - DISMISSED
  - Consumer Legal Remedies Act (Cal.) – SURVIVED (barely)
  - Unfair Competition (Cal. Bus. & Profs. Code § 17200) - SURVIVED

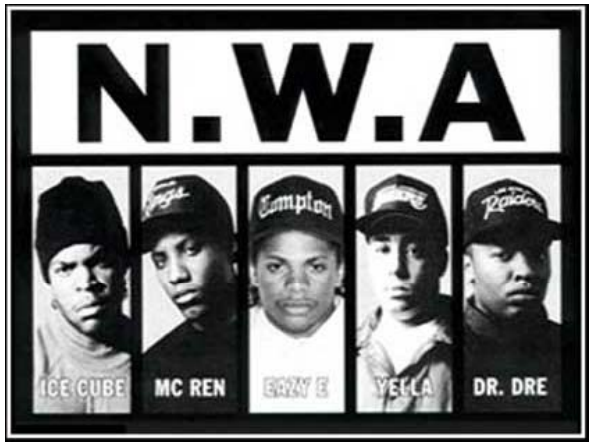
Filming the Police

A “Mobile Spring”

Filming the Police

A camera in every pocket

- “Right about now, NWA court is in full effect.
- Judge Dre presiding in the case of NWA versus the police department.
- Prosecuting attorneys are MC Ren, Ice Cube and Eazy muthafuckin E.
- Order order order. Ice Cube take the muthafuckin stand.
- Do you swear to tell the truth the whole truth and nothin but the truth so help your black ass?”

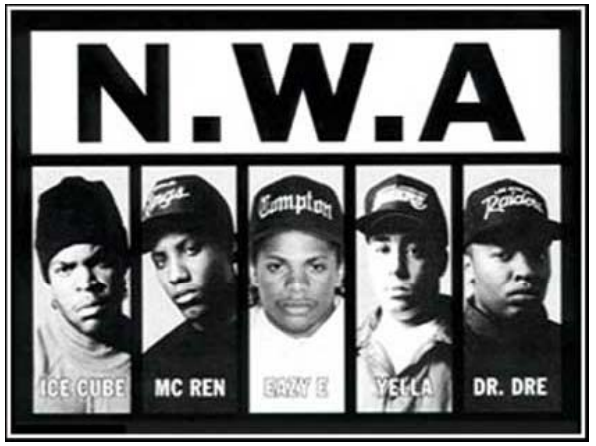


Filming the Police

A camera in every pocket

[MC Ren]
What the fuck you pulling me over for?
[Dr.Dre]
Cause I feel like it, Just sit your ass on the curb and shut the fuck up
[MC Ren]
Man, fuck this shit
[Dr.Dre]
Alright smartass, I'm taking your black ass
to jail.

M. C. Ren, will you please give your **testimony** to the jury about this fucked up incident?



Filming the Police

A camera in every pocket

- What testimony?

Filming the Police

A camera in every pocket

- What testimony?

Filming the Police

http://www.youtube.com/watch?v=jW799njhxAM

http://www.youtube.com/watch?v=40nNiXYPGs4

http://www.youtube.com/watch?v=a7ZkFZkejv8

http://www.pixiq.com/article/rochester-police-arrest-woman-for-videotaping-them

http://www.youtube.com/watch?v=tkyWA0tEkpo

http://cityroom.blogs.nytimes.com/2012/04/30/in-suit-protesters-say-city-violated-their-constitutional-rights/

Filming the Police

A camera in every pocket

- It’s not all bad…
- Cops who get it.

http://www.youtube.com/watch?v=71abF8uzW7Q

"The Redmond Police Department recognizes that citizens may record or photograph police activities in public as long as they remain at a reasonable distance, don't interfere with the employee's duties and responsibilities, and do not create a safety concern for the employee, person detained, or other persons," Gibson wrote. "The Redmond Police Department acknowledges the public has a right to record the activities of their police and that we are subject to public scrutiny as we carry out our duties to the citizens of Redmond."

http://redmond.patch.com/articles/redmond-chief-public-has-a-right-to-record-interactions-with-police#youtube_video-10110166

“Well, it should look good on YouTube…make sure you get a good picture of me…”

http://www.youtube.com/watch?v=WMMPV4D6cs0

http://www.techdirt.com/articles/20110725/17451715249/how-should-law-enforcement-handle-being-filmed-officer-lyons-provides-perfect-example.shtml

Filming the Police

A camera in every pocket

- **Sgt. Arrests Video-Taker; IA Probe Begins (June 2012)**

Filming the Police

A camera in every pocket

- But: New Haven Department of Police Service – General Order 311 (February 2011):
  - "It is the policy of the New Haven Department of Police Service to permit video recording of police activity as long as such recording does not interfere with ongoing police activity or jeopardize the safety of the general public or the police."
  - "The mere act of video recording officers of the New Haven Department of Police Service engaged in their official duties is not prohibited by federal or state statute, New Haven municipal ordinance or case law."
  - "As a result, a person may video record officers of the New Haven Department of Police Service performing their official duties, as long as such video recording does not interfere with ongoing police activity or jeopardize the safety of the general public or the police."

Filming the Police

A camera in every pocket

- How do we fight speech (videos) we don’t like?
- We provide more speech (videos)…

Minneapolis PD's own video:

http://www.onthemedia.org/2012/jun/15/minneapolis-police-filming-their-own-work/

Filming the Police

A camera in every pocket

- Apps to help
  - Qik, Bambuser – offer streaming directly to cloud storage/off-device servers
- ACLU Apps
  - "Police Tape" - http://www.nydailynews.com/new-york/new-jersey-residents-app-lets-a-spy-eye-police-article-1.1107177
  - "Stop & Frisk Watch" - http://www.nydailynews.com/new-york/new-york-civil-liberties-union-smartphone-app-lets-users-report-stop-and-frisk-encounters-real-time-article-1.1091252
- Other resources
  - http://gizmodo.com/5900680/7-rules-for-recording-police

Filming the Police

A camera in every pocket

- "Police Tape" by ACLU of New Jersey
  - "Citizens can hold police accountable in the palms of their hands with "Police Tape," a smartphone application from the ACLU of New Jersey that allows people to **securely and discreetly** record and store interactions with police, as well as provide legal information about citizens' rights when interacting with the police. Thanks to the generosity of app developer OpenWatch, the ACLU-NJ is providing Police Tape to the public free of charge." (emphasis added)
    - http://www.aclu-nj.org/yourrights/the-app-place/

Filming the Police

A camera in every pocket

- "Police Tape" – iOS version coming soon, but:
  - Is this unauthorized? iOS Developer Agreement:
    - "3.3.8 Any form of user or device data collection, or image, picture or voice capture or recording (collectively "Recordings"), and any form of data, content or information collection, processing, maintenance, uploading, syncing, storage, transmission, sharing, disclosure or use performed by, through or in connection with Your Application must comply with all applicable privacy laws and regulations as well as any related Program Requirements, including but not limited to any notice or consent requirements**. In particular, a reasonably conspicuous audio, visual or other indicator must be displayed to the user as part of the Application to indicate that a Recording is taking place**."

ACLU

AMERICAN CIVIL LIBERTIES UNION of NEW JERSEY

POLICE TAPE

Know Your Rights

Record Audio

Record Video

www.openwatch.net

ACLU

AMERICAN CIVIL LIBERTIES UNION of NEW JERSEY

Know Your Rights

Car Home Stop Arrest

If You're Stopped In Your Car

- Upon request, show them your driver's license, registration, and proof of insurance. In certain cases, your car can be searched without a warrant as long as the police have probable cause. To protect yourself later, you should make it clear that you do not consent to a search. It is not lawful for police to arrest you simply for refusing to consent to a search.
- If you're given a ticket, you

“Stop & Frisk Watch” by ACLU of New York

-Similar to “Police Tape” by ACLU of New Jersey

-Currently for Android devices only; iOS version coming soon.

http://www.nyclu.org/app

Filming the Police

Problems

Eavesdropping Statutes – ruining the party?

Filming the Police

Recent (and other) Cases

- *Glik v. Cunniffe*, 655 F.3d 78 (1st Cir. 2011) (addressed *infra*)
- *ACLU v. Alvarez*, 679 F.3d 583 (7th Cir. 2012) (addressed *infra*)
- *Smith v. City of Cumming*, 212 F.3d 1332 (11th Cir. 2000) ("The First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest")
- *Fordyce v. City of Seattle*, 55 F.3d 436 (9th Cir. 1995) (recognizing the "First Amendment right to film matters of public interest," but officer entitled to qualified immunity because Washington law was not yet settled regarding whether or not taping private conversations in public violated the eavesdropping statute)
- *Kelly v. Borough of Carlisle*, 622 F.3d 248 (3d Cir. 2010) (right to record traffic stops not "clearly established" in 3d Circuit, thus officers entitled to qualified immunity for §1983 claim)
- Department of Justice letter

Filming the Police

Glik v. Cunniffe, 655 F.3d 78 (1st Cir. 2011)

- Massachusetts: Mass. Gen. Laws ch. 272, § 99(C)(1)
- C. Offenses.
- 1. Interception, oral communications prohibited.
- Except as otherwise specifically provided in this section any person who—willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment. Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.

Filming the Police

Glik v. Cunniffe, 655 F.3d 78 (1st Cir. 2011)

- First Amendment
  - The filming of government officials engaged in their duties in a public place, including police officers performing their responsibilities, fits comfortably within these principles. Gathering information about government officials in a form that can readily be disseminated to others serves a cardinal First Amendment interest in protecting and promoting "the free discussion of governmental affairs." *Mills v. Alabama,* 384 U.S. 214, 218, 86 S.Ct. 1434, 16 L.Ed.2d 484 (1966).
  - "In our society, police officers are expected to endure significant burdens caused by citizens' exercise of their First Amendment rights. *See City of Houston v. Hill,* 482 U.S. 451, 461, 107 S.Ct. 2502, 96 L.Ed.2d 398 (1987)…"

- Fourth Amendment
  - "We thus conclude, on the facts of the complaint, that Glik's recording was not "secret" within the meaning of Massachusetts's wiretap statute, and therefore the officers lacked probable cause to arrest him. Accordingly, the complaint makes out a violation of Glik's Fourth Amendment rights."
  - Would use of ACLU apps have changed this outcome?

Filming the Police

ACLU v. Alvarez, 679 F.3d 583 (7th Cir. 2012)

- Illinois: 720 ILCS 5/14–2(a)(1)
- Sec. 14-2. Elements of the offense; affirmative defense.
- (a) A person commits eavesdropping when he:
- (1) Knowingly and intentionally uses an eavesdropping device for the purpose of hearing or recording all or any part of any conversation or intercepts, retains, or transcribes electronic communication unless he does so (A) with the **consent of all of the parties** to such conversation or electronic communication …

Filming the Police

ACLU v. Alvarez, 679 F.3d 583 (7th Cir. 2012)

- The Court analogized that just as "banning photography or note-taking at a public event would raise serious First Amendment concerns [because] a law of that sort would obviously affect the right to publish the resulting photograph or disseminate a report derived from the notes," so too does a ban on audio and audiovisual recording.
- "Restricting the use of an audio or audiovisual recording device suppresses speech just as effectively as restricting the dissemination of the resulting recording."
- "Any way you look at it, the eavesdropping statute burdens speech and press rights and is subject to heightened First Amendment scrutiny."
- "the eavesdropping statute is not closely tailored to the government's interest in protecting conversational privacy," and, as such, is likely unconstitutional
- Posner's Dissent

Filming the Police

Recent (and other) Cases

- Illinois State Case – heard one week after 7th Circuit heard the *ACLU v. Alvarez* case.
- Michael Allison – potential for 75 years prison time for secretly filming police and judge.
- Judge dismissed all eavesdropping counts.
  - "A statute intended to prevent unwarranted intrusions into a citizen's privacy cannot be used as a shield for public officials who cannot assert a comparable right of privacy in their public duties."
  - http://www.youtube.com/watch?v=80DbxSZ_FB8
  - http://www.rcfp.org/node/98367

Filming the Police

Recent (and other) Cases

- Department of Justice letter:
- "While we take no position on Mr. Sharp's claim for damages against the individual defendants, it is the United States' position that **any resolution to Mr. Sharp's claims for injunctive relief should include policy and training requirements that are consistent with the important First, Fourth and Fourteenth Amendment rights** at stake when individuals record police officers in the public discharge of their duties. **These rights, subject to narrowly-defined restrictions, engender public confidence in our police departments, promote public access to information necessary to hold our governmental officers accountable**, and ensure public and officer safety."

Filming the Police

Efforts to Ease the Tension Between the First Amendment and Eavesdropping Statutes

- Bill to amend Illinois eavesdropping statute:
  - http://www.ilga.gov/legislation/BillStatus.asp?DocTypeID=SB&DocNum=1808&GAID=11&SessionID=84&LegID=57862
  - (q) A person who is not a law enforcement officer nor acting at the direction of a law enforcement officer **may record the conversation of a law enforcement officer who is performing a public duty in a public place and any other person who is having a conversation with that law enforcement officer if the conversation is at a volume audible to the unassisted ear of the person who is making the recording**. For purposes of this subsection (q), "public place" means any place to which the public has access and includes, but is not limited to, streets, sidewalks, parks, and highways (including inside motor vehicles), and the common areas of public and private facilities and buildings.
  - Is Judge Posner's concern about the citizen's privacy when talking with the police a valid concern?

Filming the Police

Efforts to Ease the Tension Between the First Amendment and Eavesdropping Statutes

- Bill to amend Connecticut eavesdropping statute:
  - http://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00245&which_year=2012
- (b) A peace officer who interferes with any person taking a photographic or digital still or video image of such peace officer or another peace officer acting in the performance of such peace officer's duties shall, subject to sections 5-141d, 7-465 and 29-8a of the general statutes, be liable to such person in an action at law, suit in equity or other proper proceeding for redress.
- (c) A peace officer shall not be liable under subsection (b) of this section if the peace officer had reasonable grounds to believe that the peace officer was interfering with the taking of such image in order to (1) lawfully enforce a criminal law of this state or a municipal ordinance, (2) protect the public safety, (3) preserve the integrity of a crime scene or criminal investigation, (4) safeguard the privacy interests of any person, including a victim of a crime, or (5) lawfully enforce court rules and policies of the Judicial Branch with respect to taking a photograph, videotaping or otherwise recording an image in facilities of the Judicial Branch.
- http://www.pixiq.com/article/connecticut-senate-approves-bill

Misc. Mobile Privacy Issues

Self Encryptination

Self Encryptination

- *In RE: GRAND JURY SUBPOENA DUCES TECUM DATED MARCH 25, 2011* (11th Cir. February 23, 2012)
- Defendant ordered to produce contents of encrypted hard drives.
- Defendant indicated he would invoke Fifth Amendment privilege against self-incrimination.
- District court granted Defendant immunity for act of decrypting but not for contents of drives. Defendant argued that that simply accomplished derivative use of the immunized testimony (decrypting the drives).
- Defendant refused. Criminal contempt.

Self Encryptination

- On appeal:
- "For the reasons that follow, we hold that Doe's decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government's use of the drives' contents. The district court therefore erred in two respects.

- First, it **erred in concluding that Doe's act of decryption and production would not constitute testimony**.

- Second, in granting Doe immunity, it **erred in limiting his immunity**, under 18 U.S.C. §§ 6002 and 6003, to the Government's use of his act of decryption and production, but allowing the Government derivative use of the evidence such act disclosed."

Self Encryptination

- On appeal:
- With encrypted files, the "location, existence, and authenticity" of the purported evidence is (usually) unknown, so the contents of the individual's mind (encryption password) would be used against him.
  - *See Fisher v. United States,* 425 U.S. 391 (1976) and *United States v. Hubbell,* 530 U.S. 27 (2000).
- "We reach this holding by concluding that (1) Doe's decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit factual communications associated with the decryption and production are not foregone conclusions."

Self Encryptination

- *United States v. Fricosu* (D. Colo. January 23, 2012) – Order requiring Fricosu to decrypt a laptop hard drive.
- "There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production." (There were tapes with Fricosu talking about the files.)
- "Accordingly, I find and conclude that the Fifth Amendment is not implicated by requiring production of the unencrypted contents of the Toshiba Satellite M305 laptop computer." (Note, Fricosu has to provide an unencrypted drive, not the password to decrypt.)
- "Moreover, the government has offered Ms. Fricosu immunity, precluding it from using her act of producing the unencrypted contents of the laptop computer against her…Accordingly, the writ should issue."

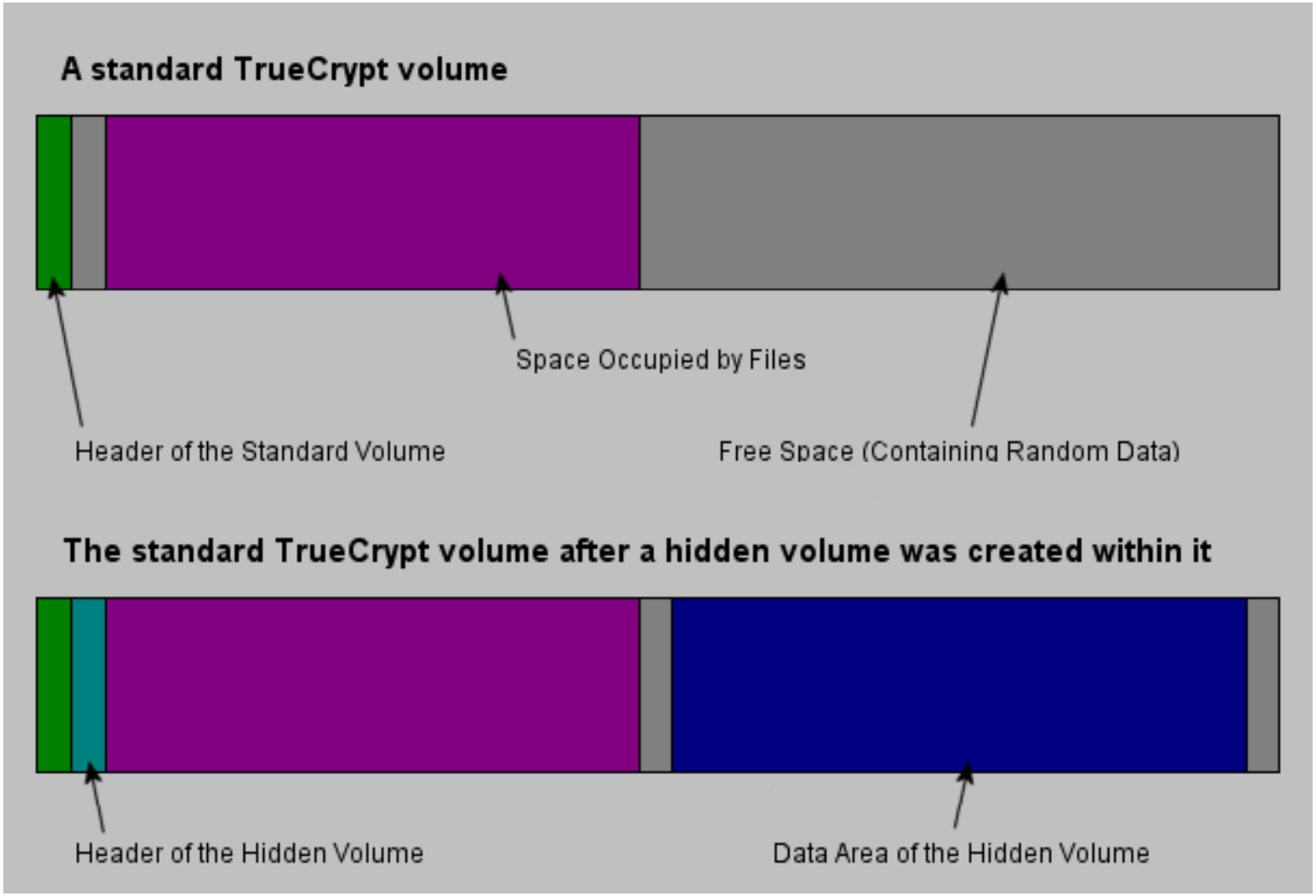
Self Encryptination

- 10th/11th Circuit split avoided?
- Co-defendant may have provided password. Laptop has been decrypted without Fricosu's aid.
- But, 11th Circuit cited the Fricosu order in a footnote: "Throughout this extensive exchange [the phone calls], Fricosu essentially admitted every testimonial communication that may have been implicit in the production of the unencrypted contents. Here, in contrast, the Government does not know whether any files are present on the encrypted drive; whether Doe has access to and control over the encrypted drives; and whether Doe is capable of decryption."

Self Encryptination

- TrueCrypt
- Use with USB drives or other drives
- http://www.truecrypt.org
  - http://www.truecrypt.org/docs/?s=plausible-deniability
  - “Plausible Deniability” feature creates ability for “fake” password to open honeypot/bogus volume.
  - But, is failure to disclose the “real” password perjury?

Self Encryptination



Requests for Mobile Phone Data

- July 9, 2012
- WASHINGTON, D.C. – In the first-ever accounting of its kind, Congressman Edward J. Markey (D-Mass) has found that in 2011, federal, state and local law enforcement agencies made more than 1.3 million requests of wireless carriers for the cell phone records of consumers, and that number is increasing every year. Last month, Rep. Markey queried nine mobile wireless carriers about their policies and practices for sharing their customers' mobile phone information with law enforcement agencies after a report in the New York Times reported that law enforcement was routinely requesting consumers cell phone records, sometimes with little judicial oversight and no consumer knowledge. The responses received by Rep. Markey were startling in the volume and scope of requests made by law enforcement, including requests for "cell tower dumps" in which carriers provide all the phones numbers of cell users that connect with a tower during a discreet period of time, including information on innocent people. According to the carriers, all requests were made pursuant to a legal warrant or granted due to an emergency situation in which an individual was in imminent danger.
  - http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers

Requests for Mobile Phone Data

- **More Demands on Cell Carriers in Surveillance:** http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all
- **Letters to mobile carriers regarding use of cell phone tracking by law enforcement:** http://markey.house.gov/content/letters-mobile-carriers-reagrding-use-cell-phone-tracking-law-enforcement

Takeaways

- FTC continuing to show interest in apps.
- Cameras in every pocket helping solidify First Amendment protection for filming public officials on duty.
- Enterprising app developers also helping exercise those rights – but be careful…
- …Eavesdropping statutes may still conflict with First Amendment, despite increasingly good case law.
- The tech savvy will rule the Earth – keep your passwords strong, and your encryption stronger.

Kevin W. Wimberly
kevin@firstamendment.com