Copyright and Your Rights

The author retains the copyright in this book. By downloading a copy of this book from the Semaphore Press website, you have made an authorized copy of the book from the website for your personal use. If you lose it, or your computer crashes or is stolen, don’t worry. Come back to the Semaphore Press website and download a replacement copy, and don’t worry about having to pay again. Just to be clear, Semaphore Press and the author of this casebook are not granting you permission to reproduce the material and books available on our website except to the extent needed for your personal use. We are not granting you permission to distribute copies either.

We ask that you not resell or give away your copy. Please direct people who are interested in obtaining a copy to the Semaphore Press website, www.semaphore-press.com, where they can download their own copies. The resale market in the traditional casebook publishing world is part of what drives casebook prices up to $200 or more. When a publisher prices a book at $200, it is factoring in the competition and lost opportunities that the resold books embody for it. Things are different at Semaphore Press: Because anyone can get his or her own copy of a Semaphore Press book at a reasonable price, we ask that you help us keep legal casebook materials available at reasonable prices by directing anyone interested in this book to our website.

Printing A Paper Copy

If you would like to have a printed copy of the book in addition to the electronic copy, you are welcome to print out a copy of any part, or all, of the book. Please note that you will find blank pages throughout the book. We have inserted these intentionally to facilitate double-sided printing. We anticipate that students may wish to carry only portions of the book at a time. The blank pages are inserted so that each chapter begins on a fresh, top-side page. Printed copies of the full book are also available through Amazon.com.

Finding Aids and Annotations

Finally, please note that the book does not include an index, a table of cases, or other finding aids that are conventional for printed books. This is because a Semaphore Press book, in pdf form, can be searched electronically for any word or phrase in which you are interested. With the book open in Adobe Reader, simply hit control-f (or select the "find" option in the "Edit" pull-down menu) and enter the search term you want to find. We also enable Reader’s commenting features in our pdf books, so you can highlight text, insert comments, and personally annotate your copy in other ways you find helpful. If your copy of Reader does not appear to permit these commenting features, please check to make sure you have the most recent version; any version numbered "8" or higher should permit you to annotate a Semaphore Press book.

For my parents.
INTERNET LAW: CASES AND PROBLEMS

INTRODUCTION ........................................................................................................9

CHAPTER 1: BACKGROUND ...............................................................................17
A. Computer Technology ..................................................................................17
   Technical Primer: Computers .......................................................................17
   Technical Primer: The Internet ..................................................................27
   Columbia Pictures Indus. v. Fung ...............................................................36
   Internet Applications Problem .................................................................39
B. Theory ...........................................................................................................40
   Code 2.0 .......................................................................................................40
   The Future of the Internet .........................................................................44

CHAPTER 2: JURISDICTION ............................................................................51
A. Cyberspace ...................................................................................................51
   A Declaration of the Independence of Cyberspace ....................................51
   The Problem of Perspective in Internet Law .............................................53
   Law and Borders .......................................................................................55
   Unwilling Avatars .....................................................................................58
   Voyeur Dorm L.C. v. City of Tampa ..........................................................61
   Voyeur Dorm L.C. v. City of Tampa ..........................................................62
   National Federation of the Blind v. Target Corp. ......................................63
   Dead Aim Problem ...................................................................................67
B. Territoriality ..................................................................................................68
   Dow Jones & Co. v. Gutnick .......................................................................69
   Mahfouz v. Ehrenfeld ...............................................................................75
   Note on the Dormant Commerce Clause ...............................................77
   Overstock.com v. New York State Dept. of Taxation and Finance ..........79
   Diplomatic Mission Problem ...................................................................82
C. Enforcement ..................................................................................................83
   SPEECH Act .............................................................................................83
   Note on Extradition ..................................................................................84
   Google Inc. v. Equustek Solutions Inc. .....................................................85
   Digital Borders .........................................................................................91
   SeaHaven Problem ..................................................................................95
   Gambling Treaty Problem .......................................................................96
D. Personal Jurisdiction and Venue .................................................................97
   Burdick v. Superior Court ........................................................................99
   Penguin Group (USA) Inc. v. American Buddha ......................................107
   United States v. Auernheimer .................................................................111
   Too Damn High Problem .......................................................................116
   FloodZone Problem ...............................................................................116

CHAPTER 3: SPEECH .....................................................................................119
A. Defining “Speech” .......................................................................................119
   United States Constitution, Amendment I ..............................................119
   Texas v. Johnson .....................................................................................119
   Bland v. Roberts .....................................................................................120
   Bland v. Roberts .....................................................................................122
Pen Registers and Trap and Trace Devices ................................................................. 258
Note on technical Assistance .................................................................................. 260
C. National Security .................................................................................................. 261
   Liberty and Security in a Changing World ............................................................ 262
   Other Surveillance Programs .................................................................................. 268
   Legal Challenges to NSA Surveillance ................................................................ 270
   Zipper Problem .................................................................................................... 272
D. Anonymity ............................................................................................................. 273
   Stored Communications Act .................................................................................. 274
   Jukt Micronics Problem ....................................................................................... 274
   Doe I v. Individuals, Whose True Names Are Unknown ........................................ 275
E. Consumer Privacy ................................................................................................ 280
   In re DoubleClick Inc. Privacy Litig ....................................................................... 280
   In re Google, Inc. Privacy Policy Litig. ................................................................. 286
   In re Snapchat, Inc. .............................................................................................. 296
   Cookie Monster Problem ...................................................................................... 302
F. An International Perspective ................................................................................ 303
   Data Protection Directive ...................................................................................... 303
   European Union: ECJ Invalidates Data Retention Directive ............................... 306
   Google Spain SP v. Agencia Española de Protección de Datos ....................... 308
   Schrems v. Data Protection Commissioner .......................................................... 314

CHAPTER 5: ACCESS TO COMPUTERS .................................................................. 323
A. Contracts ............................................................................................................... 323
   CX Digital Media, Inc. v. Smoking Everywhere, Inc ............................................ 323
   Nguyen v. Barnes & Noble, Inc. ........................................................................... 330
   Smurfberry Problem ............................................................................................. 335
   ProCD, Inc. v. Zeidenberg .................................................................................... 336
   Krustilu Problem .................................................................................................. 337
   SeaSells Problem ................................................................................................. 337
B. Computer Misuse Statutes .................................................................................... 338
   Computer Fraud and Abuse Act ........................................................................... 338
   United States v. Morris ......................................................................................... 340
   United States v. Nosal [I] .................................................................................... 342
   United States v. Nosal [II] ................................................................................... 349
C. Trespass to Chattels .............................................................................................. 351
   Restatement (Second) of Torts [trespass] .......................................................... 352
   Intel v. Hamidi ...................................................................................................... 352
   Note on Spam ....................................................................................................... 359
   Wireless Router Problem ..................................................................................... 361
   LineJump Problem ............................................................................................. 361

CHAPTER 6: TRADEMARKS & DOMAIN NAMES .............................................. 363
A. Trademark Basics ................................................................................................ 363
   Multi Time Machine, Inc. v. Amazon. com, Inc .................................................. 364
   Tiffany (NJ) Inc. v. eBay, Inc .............................................................................. 373
   Happy Fun Ball Problem ..................................................................................... 379
B. Domain Names ....................................................................................................... 380
   Title 15, United States Code ............................................................................... 381
   Taubman Co. v. Webfeats ................................................................................... 383
CHAPTER 7: COPYRIGHT .................................................................................. 405
Copyright Overview ..................................................................................... 405
A. The Exclusive Rights ................................................................................ 407
   Copyright Act [Exclusive Rights and First Sale] ....................................... 407
   Capitol Records, LLC v. ReDigi, Inc. ......................................................... 408
   Note on RAM Copies ................................................................................ 414
   Perfect 10, Inc. v. Amazon.com, Inc. ......................................................... 415
   American Broadcasting Co. v. Aereo, Inc. ................................................ 419
   Music Locker Problem .............................................................................. 422
B. Licenses .................................................................................................... 422
   Field v. Google Inc. .................................................................................. 423
   Vernor v. Autodesk, Inc. .......................................................................... 428
   MIT License ............................................................................................. 433
   GNU General Public License (GPL) ......................................................... 434
   Jacobsen v. Katzer ................................................................................... 438
C. Fair Use .................................................................................................... 443
   Copyright Act [Fair Use] .......................................................................... 443
   Note on Sony v. Universal (Fair Use) ......................................................... 444
   A & M Records, Inc. v. Napster, Inc. ......................................................... 445
   Katz v. Google Inc. .................................................................................. 449
   Perfect 10, Inc. v. Amazon.com, Inc. ......................................................... 453
   Bubonic Plagiarism Problem .................................................................... 456
D. Direct and Secondary Liability ................................................................. 457
   Perfect 10, Inc. v. Giganews, Inc. ............................................................. 457
   Note on Sony v. Universal (Contributory Infringement) ............................ 461
   A & M Records, Inc. v. Napster, Inc. ......................................................... 462
   Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. .............................. 466
   Cachet Problem ...................................................................................... 471
   Rip-Mix-Burn Problem .......................................................................... 472
E. Section 512 ............................................................................................. 473
   Copyright Act [Section 512] .................................................................... 473
   Friday Problem ....................................................................................... 478
   Lenz v. Universal Music Corp. ................................................................. 478
   Perfect 10, Inc. v. CCBill LLC ................................................................. 484
   Section 512 Compliance Questions .......................................................... 488
   Materials on Content ID .......................................................................... 489
   Mangle Problem ...................................................................................... 496
F. Digital Rights Management ..................................................................... 497
   Note on Digital Rights Management ....................................................... 497
   Note on the Motivation for Anti-Circumvention Law ............................... 498
   Copyright Act [Anti-Circumvention] .......................................................... 499
   Universal City Studios, Inc. v. Corley ...................................................... 500
   Universal City Studios, Inc. v. Reimerdes ............................................... 502
| Section 1201 Problems ....................................................................................... | 508 |
| Note on DMCA Exemptions .................................................................................. | 509 |

| CHAPTER 8: PATENT ......................................................................................... | 511 |
| Alice Corp. v. CLS Bank Int’l ......................................................................... | 511 |
| Soverain Software LLC v. Newegg Inc. ............................................................ | 519 |
| Function Media, L.L.C. v. Google ................................................................. | 524 |
| Apple v. Motorola ............................................................................................ | 528 |
| Apple v. Motorola ............................................................................................ | 530 |

| CHAPTER 9: PRIVATE POWER ........................................................................... | 533 |
| A. First Amendment Limits ............................................................................. | 533 |
| Cyber Promotions, Inc. v. American Online, Inc. ........................................... | 533 |
| Zhang v. Baidu.com Inc .................................................................................. | 537 |
| WikiLeaks Problem .......................................................................................... | 544 |
| CurrenC Problem ............................................................................................ | 546 |
| Spam Posse Problem ...................................................................................... | 546 |
| B. Antitrust ................................................................................................. | 547 |
| Note on Antitrust Law and Economics ......................................................... | 547 |
| United States v. Microsoft Corp. .................................................................... | 549 |
| LiveUniverse, Inc. v. MySpace, Inc. .............................................................. | 556 |
| Google Maps Problem .................................................................................... | 562 |
| C. Network Neutrality ................................................................................... | 563 |
| Verizon v. FCC .............................................................................................. | 563 |
| Note on Administrative Law ......................................................................... | 567 |
| Note on Telephone Regulation ..................................................................... | 569 |
| Broadband Internet Regulation: A Brief History ......................................... | 573 |
| Note on Wireless Regulation ....................................................................... | 583 |
| Note on Interconnection ............................................................................. | 585 |
| Protecting and Promoting the Open Internet ............................................. | 587 |
| Dissenting Statement of Commissioner Ajit Pai .......................................... | 596 |
| DoubleNet Problem ....................................................................................... | 601 |
| The punchline? ............................................................................................. | 602 |

| CHAPTER 10: BEYOND THE INTERNET ......................................................... | 603 |
| A. Virtual Property ...................................................................................... | 603 |
| Kremen v. Cohen ............................................................................................ | 603 |
| United States v. Aleynikov .......................................................................... | 609 |
| Bragg v. Linden Research, Inc ...................................................................... | 614 |
| Note on Bitcoin ............................................................................................ | 626 |
| United States v. Ulbricht ............................................................................. | 629 |
| Digital Currency Regulatory Guidance ...................................................... | 632 |
| Slot Machine Problem ................................................................................. | 634 |
| Post.Mortem Problem .................................................................................. | 635 |
| Davy Jones Problem .................................................................................... | 635 |
| B. Defective Software ................................................................................... | 636 |
| Kennison v. Daire .......................................................................................... | 636 |
| Pompeii Estates, Inc. v. Consolidated Edison Co. of N.Y., Inc. .................. | 637 |
| Rosenberg v. Harwood .................................................................................. | 640 |
CHAPTER 4: PRIVACY

This chapter explores the vexed problem of online privacy. On the one hand, the Internet seems to offer new and unprecedented opportunities for interacting discreetly. As a dog in a *New Yorker* cartoon famously put it, “On the Internet, nobody knows you’re a dog.” On the other hand, online activities leave behind a trail of data in the hands of websites, ISPs, and others. That trail can be used to identify individual users, and in some cases to build detailed profiles of what they have been doing.

The first half of the chapter focuses on criminal investigations, examining constitutional and statutory restrictions on how law enforcement can gain access to individuals’ data. Governmental control provides the thematic backbone. The second half then shifts to the problem of what private parties know and can learn about Internet users. Here, intermediary power comes to the fore: if knowledge is power, then these intermediaries have quite a lot, indeed.

A. The Fourth and Fifth Amendments

We begin with criminal procedure: the body of law that regulates investigation, prosecution, and criminal trials. The overriding concern here is evidentiary. The police are looking to gather evidence that can be used against a defendant at trial; the defendant is looking either to keep the police from getting access to the evidence, or to keep the prosecutors from presenting it to the jury. The Fourth Amendment exclusionary rule provides the legal backdrop for this struggle: police must respect the defendant’s privacy rights during the investigation, or the resulting evidence will be inadmissible. It fits together with the Fifth Amendment, which prevents the police from shortcutting their own investigation by compelling the defendant to tell the complete story of what happened.

This section considers how the Fourth and Fifth Amendments apply when there are computers involved. *Riley v. California* introduces the ways in which computers may be meaningfully different from other objects the police search; *United States v. Warshak* brings third parties into the picture and asks what happens to information as it travels on the Internet. *United States v. Doe* asks how the Fifth Amendment applies to encrypted data protected by a password.

**FOURTH AND FIFTH AMENDMENT OVERVIEW**

The Fourth Amendment reads:

> 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.

At the outset, two threshold issues are particularly important. First, only searches by the government implicate the Fourth Amendment; it does not apply to “a

* The cartoon, by Peter Steiner, appeared on page 61 of the July 5, 1993 issue.
search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.” United States v. Jacobsen, 466 U.S. 109, 114 (1984). If a FedEx clerk opens your wrapped package and drugs tumble out, this is a “private search” and the Fourth Amendment is uninterested. Indeed, the clerk can take the package to the police to show them what he found. Second, unless the governmental action violates your “reasonable expectation of privacy,” no “search” has taken place. If a police officer sees you run out of a bank wearing a ski mask and waving a gun, the officer’s act of looking at you is not a “search” for Fourth Amendment purposes, and the officer is free to testify at trial that she saw you leaving the bank – or to arrest you.

The “reasonable expectation of privacy” test comes from Katz v. United States, 389 U.S. 347 (1967). There, the police bugged a phone booth they knew the defendant regularly used; the Supreme Court held that this constituted a search. Katz was a watershed in criminal procedure; it repudiated older cases holding that there was no search without an “actual physical invasion” of a defendant’s property. Olmstead v. United States, 277 U.S. 438, 466 (1928). Katz shifted the focus of the Fourth Amendment from spaces and objects protected against trespassers to “expectation[s] of privacy … that society is prepared to recognize as reasonable.” Katz, 389 U.S. at 361 (Harlan, J., concurring).

Drawing the line that defines a “reasonable expectation of privacy” is extremely hard, but a few examples are relatively clear. You have a reasonable expectation of privacy in your home and in sealed containers, such as locked suitcases within your control. By contrast, you have no reasonable expectation of privacy in anything you have voluntarily exposed to public view.

Complicating the issue, the Fourth Amendment prohibits only “unreasonable” searches and seizures. A search is automatically reasonable if it is carried out pursuant to a search warrant: a judicial order that gives the police permission to carry out the search. A court can issue a warrant after the police provide “probable cause,” i.e., “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). It must also specify which particular places are to be searched or which items are to be seized; a search or seizure that goes beyond those limits is invalid.

Some warrantless searches can still be “reasonable” and thus permissible. Some of these exceptions (each of which has its own tests) would take us well outside the scope of this course – at the U.S. border, in government workplaces, in schools and prisons, and as part of a lawful stop or arrest. The police may also conduct warrantless searches and seizures when “exigent circumstances” make obtaining a warrant infeasible – most commonly, when there is a risk that evidence will be destroyed if they do not act. An unreasonable search is illegal, and the “exclusionary rule” governs any evidence the police obtain as a result: it may not be introduced at trial.

Two other exceptions are important for our purposes. First, there’s the “consent” exception: if the owner or someone else with authority over the property consents, the police may search it. If you invite the police into your basement meth lab, you may not later argue that it was a private space they needed a warrant to enter. The same goes if your housemate invites them into the shared meth lab. The second is the “plain view” rule. If the police are executing a valid search warrant, they may also search and seize evidence whose incriminating nature is “immediately apparent.” If the police are searching the basement meth lab pursuant to a
valid warrant, they can also follow the trail of blood up the stairs. These two exceptions have a lot in common with the basic reasonable expectation of privacy test. Can you articulate a general principle that unites them?

The Fourth Amendment also applies to “seizures.” A seizure of your person is an arrest or other involuntary restriction of your liberty to leave. A seizure of your property takes place when there is “some meaningful interference with [your] possessory interest.” United States v. Jacobsen, 466 U.S. 109, 113 (1984). Again, a search warrant, issued by a judge, with a probable-cause standard of evidence, and particularly describing who or what is to be seized, is ordinarily required.

The Fifth Amendment provides:

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself; nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation. (emphasis added)

This is the familiar “right to remain silent”: a criminal defendant has an absolute privilege to refuse to testify. She is also free to refuse to answer questions from police, grand juries, even Congress – anything that might potentially incriminate her. The government can compel her testimony only by offering the defendant immunity: a promise that neither the testimony, nor anything discovered using the testimony, will be used against the defendant at trial. Some of the hard questions, as United States v. Doe illustrates, depend on the question of what actions count as “testimony.”

NOTE ON WARRANT JURISDICTION

Another important limit on search warrants is that they are only valid where the issuing court has territorial authority. In a world where most crimes are planned and committed locally and where most search warrants describe houses and other buildings, this last constraint is rarely likely to pose an obstacle. But modern technologies create difficulties. For example, cars drive around. In United States v. Jones (discussed below), investigators obtained a warrant to install a GPS tracker on the defendant’s car from a federal court in the District of Columbia but actually installed the tracker in Maryland. Whoops. (This is why the case reached the Supreme Court as a case on whether a warrant was necessary at all.)

Computers pose even more vexing issues. In one notable case, the FBI took over a child pornography website and used it to install tracking software on the computers of users who visited it so they could be identified and prosecuted. It obtained a warrant from a magistrate judge in the Eastern District of Virginia allowing a search of the “computers ... of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.” But those computers were located all over the United States. Judges in the resulting prosecutions split over whether the warrant was valid under the current version of the Federal Rules of Criminal Procedure, which allowed only a “magistrate judge with authority in the district” to issue a warrant. Fed. R. Crim. Proc. 41(b)(1) (emphasis added). But within the U.S. federal judicial system, where Congress controls the jurisdictional rules and can change them, such problems (if they really are prob-
lems) are solvable. An amendment to Rule 41 that explicitly authorized nationwide warrants in such cases went into effect on December 1, 2016.

Internationally, the jurisdictional overlaps can be messy. If Microsoft, a U.S. company with subsidiaries and operations around the world, stores a user’s emails on a server in Ireland, can United States authorities compel Microsoft to turn over the emails? What about Irish authorities? Does it matter whether the user is American or Irish? In *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), the court held that a warrant issued by a federal court under the Stored Communications Act could not reach emails stored in Ireland. In June 2017, the government asked the Supreme Court to review the case — so perhaps this is not the last word.

**NOTE ON UNITED STATES V. JONES**

The Supreme Court’s decision *United States v. Jones*, 132 S. Ct. 945 (2012), complicates this picture; although the judgment itself was unanimous, the court’s three separate opinions took wildly different approaches to the Fourth Amendment. In brief, government agents police installed a GPS tracking device on Antoine Jones’s car and recorded thousands of pages of data about its movements over a 28-day period. The GPS data connected him to a stash house containing 97 kilograms of cocaine; he was convicted of conspiracy to distribute illegal drugs and sentenced to life imprisonment.

The starting point for the legal analysis was that there is generally no expectation of privacy in one’s movements in public. The police can tail you and take photographs as you go into a stash house. Two previous Supreme Court cases — *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984) — had upheld police use of more primitive tracking devices: radio transmitters, called “beepers,” that actively signaled their location to help police with the appropriate receiving equipment follow a suspect.

Justice Scalia’s majority opinion in *Jones* sidestepped the question of how the *Katz* reasonable expectation test would apply to long-term GPS tracking by holding that the agents had trespassed on Jones’s car by installing the GPS device. (In both *Knotts* and *Karo*, the beeper was installed in an object before it came into the defendant’s possession.) For the majority, *Katz* left intact the older, property-based cases:

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.

*Jones*, 132 S. Ct. at 949.

Justice Alito, concurring in the judgment for four justices, read *Katz* to have replaced “18th-century tort law” with the reasonable expectations test. Applying that test, Alito’s opinion drew a distinction based on the scale of the surveillance:

> Under this approach, relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been
that law enforcement agents and others would not – and indeed, in
the main, simply could not – secretly monitor and catalogue every sin-
gle movement of an individual’s car for a very long period. In this case,
for four weeks, law enforcement agents tracked every movement that
respondent made in the vehicle he was driving. We need not identify
with precision the point at which the tracking of this vehicle became a
search, for the line was surely crossed before the 4-week mark.

Id. at 964 (Alito, J., concurring in the judgment). This approach has become
known as the “mosaic” theory of the Fourth Amendment: the individual tiles are
trivial and uninteresting, but when assembled they become highly revealing.

But is the mosaic theory law? At the Supreme Court, not as such. Justice So-
tomayor’s concurrence expressed great sympathy for the mosaic theory but con-
cluded that it was unnecessary to resolve the “difficult questions” adopting it
would raise “because the Government’s physical intrusion on Jones’ Jeep supplies
a narrower basis for decision.” Id. at 957 (Sotomayor, J., concurring). This split
puts lower courts in an awkward position in electronic surveillance cases that lack
the easy out of a physical intrusion. Five Justices have praised the mosaic theory,
but only four have endorsed it as law in the case before them.

Here is an example of the kind of controversies now raging through the lower
courts. Under Smith v. Maryland, 442 U.S. 735 (1979) (discussed in Warshak
and the NSA cases below), the telephone numbers a defendant dials are not protected
by the Fourth Amendment under the “third party doctrine”: he voluntarily surren-
dered his privacy in them by revealing them to the phone company. But cell phone
towers also necessarily track a caller’s location so they can hand off a phone call
from one tower to the next as the phone moves around. Suppose the police are
interested in finding out where a defendant was when he made calls from his cell
phone. Do they need a warrant to obtain this “cell site location
information” (CSLI) from the defendant’s cell phone carrier? So far, the federal
Courts of Appeals have agreed that no warrant is needed. See, e.g., In re U.S. for
Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (“Cell phone users,
therefore, understand that their service providers record their location information
when they use their phones at least to the same extent that the landline users
in Smith understood that the phone company recorded the numbers they dialed.”)
Despite the absence of a circuit split, the Supreme Court agreed to hear a CSLI

RILEY V. CALIFORNIA
134 S. Ct. 2473 (2014)

Chief Justice Roberts delivered the opinion of the Court.

These two cases raise a common question: whether the police may, without a
warrant, search digital information on a cell phone seized from an individual who
has been arrested.

I

A

In the first case, petitioner David Riley was stopped by a police officer for driving
with expired registration tags. In the course of the stop, the officer also learned
that Riley’s license had been suspended. The officer impounded Riley’s car, pur-
suant to department policy, and another officer conducted an inventory search of
the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood.

An officer searched Riley incident to the arrest and found items associated with the “Bloods” street gang. He also seized a cell phone from Riley’s pants pocket. According to Riley’s uncontradicted assertion, the phone was a “smart phone,” a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters “CK”—a label that, he believed, stood for “Crip Killers,” a slang term for members of the Bloods gang.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he “went through” Riley’s phone “looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns.” Although there was “a lot of stuff” on the phone, particular files that “caught [the detective’s] eye” included videos of young men sparring while someone yelled encouragement using the moniker “Blood.” The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley was ultimately charged, in connection with that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. The State alleged that Riley had committed those crimes for the benefit of a criminal street gang, an aggravating factor that carries an enhanced sentence. Prior to trial, Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances. The trial court rejected that argument. At Riley’s trial, police officers testified about the photographs and videos found on the phone, and some of the photographs were admitted into evidence. Riley was convicted on all three counts and received an enhanced sentence of 15 years to life in prison.

The California Court of Appeal affirmed. …

The California Supreme Court denied Riley’s petition for review and we grant certiorari.

In the second case, a police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car. Officers subsequently arrested Wurie and took him to the police station. At the station, the officers seized two cell phones from Wurie’s person. The one at issue here was a “flip phone,” a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone. Five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as “my house” on the phone’s external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone’s wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the “my house” label. They next used an online phone directory to trace that phone number to an apartment building.

When the officers went to the building, they saw Wurie’s name on a mailbox and observed through a window a woman who resembled the woman in the photo-
tograph on Wurie’s phone. They secured the apartment while obtaining a search warrant and, upon later executing the warrant, found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.

Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. He moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of his cell phone. The District Court denied the motion. Wurie was convicted on all three counts and sentenced to 262 months in prison.

A divided panel of the First Circuit reversed ...

We granted certiorari.

II

The Fourth Amendment provides:

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.

As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness. Our cases have determined that where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant. Such a warrant ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.

The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest. In 1914, this Court first acknowledged in dictum “the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.” *Weeks v. United States*, 232 U.S. 383, 392 (1914). Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement. ...

Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. ... That debate has focused on the extent to which officers may search property found on or near the arrestee. Three related precedents set forth the rules governing such searches:

The first, *Chimel v. California*, 395 U.S. 752 (1969), laid the groundwork for most of the existing search incident to arrest doctrine. Police officers in that case arrested Chimel inside his home and proceeded to search his entire three-bedroom house, including the attic and garage. In particular rooms, they also looked through the contents of drawers.

The Court crafted the following rule for assessing the reasonableness of a search incident to arrest:

When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer’s safety might well be endangered, and the ar-
rest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. . . . There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control'-construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.

*Id.*, at 762-763. The extensive warrantless search of Chimel's home did not fit within this exception, because it was not needed to protect officer safety or to preserve evidence.

Four years later, in *United States v. Robinson*, 414 U.S. 218 (1973), the Court applied the *Chimel* analysis in the context of a search of the arrestee's person. A police officer had arrested Robinson for driving with a revoked license. The officer conducted a patdown search and felt an object that he could not identify in Robinson's coat pocket. He removed the object, which turned out to be a crumpled cigarette package, and opened it. Inside were 14 capsules of heroin. . . .

This Court . . . reject[ed] the notion that "case-by-case adjudication" was required to determine "whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest." . . .

The Court thus concluded that the search of Robinson was reasonable even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed.

The search incident to arrest trilogy concludes with *Arizona v. Gant*, 556 U.S. 332 (2009), which analyzed searches of an arrestee's vehicle. *Gant*, like *Robinson*, recognized that the *Chimel* concerns for officer safety and evidence preservation underlie the search incident to arrest exception. As a result, the Court concluded that *Chimel* could authorize police to search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." 556 U.S., at 343. *Gant* added, however, an independent exception for a warrantless search of a vehicle's passenger compartment "when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" *Ibid*. That exception stems not from *Chimel*, the Court explained, but from "circumstances unique to the vehicle context." 556 U.S., at 343.

III

These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. Even less sophisticated phones like Wurie's, which have already faded in popularity since Wurie was arrested in 2007, have been around for less than 15 years. Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests. Such a balancing of interests supported the search incident to arrest exception in *Robinson*, and a mechanical application of *Robinson* might well support the warrantless searches at issue here.
But while Robinson’s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, Robinson concluded that the two risks identified in Chimel – harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, Robinson regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson.

We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.

A

We first consider each Chimel concern in turn. ...

1

Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon–say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.

Perhaps the same might have been said of the cigarette pack seized from Robinson’s pocket. Once an officer gained control of the pack, it was unlikely that Robinson could have accessed the pack’s contents. But unknown physical objects may always pose risks, no matter how slight, during the tense atmosphere of a custodial arrest. The officer in Robinson testified that he could not identify the objects in the cigarette pack but knew they were not cigarettes. Given that, a further search was a reasonable protective measure. No such unknowns exist with respect to digital data. As the First Circuit explained, the officers who searched Wurie’s cell phone “knew exactly what they would find therein: data. They also knew that the data could not harm them.” ...

2

The United States and California focus primarily on the second Chimel rationale: preventing the destruction of evidence.

Both Riley and Wurie concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant. That is a sensible concession. And once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone.

The United States and California argue that information on a cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption. Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called “geofencing”). Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data be-
Internet Law

comes protected by sophisticated encryption that renders a phone all but “unbreakable” unless police know the password. ...

We have also been given little reason to believe that either problem is prevalent. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest. Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited. Law enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity. See, e.g., iPhone User Guide for iOS 7.1 Software 10 (2014) (default lock after about one minute). ...

Moreover, in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to conduct a warrantless search would make much of a difference. The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a cell phone right away. Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed, which might be at the station house hours later. Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted.

In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. Such devices are commonly called “Faraday bags,” after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use. They may not be a complete answer to the problem, but at least for now they provide a reasonable response. In fact, a number of law enforcement agencies around the country already encourage the use of Faraday bags.

To the extent that law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns. If the police are truly confronted with a now or never situation – for example, circumstances suggesting that a defendant’s phone will be the target of an imminent remote-wipe attempt – they may be able to rely on exigent circumstances to search the phone immediately. Or, if officers happen to seize a phone in an unlocked state, they may be able to disable a phone’s automatic-lock feature in order to prevent the phone from locking and encrypting data. Such a preventive measure could be analyzed under the principles set forth in our decision in McArthur, 531 U.S. 326, 331–33 (2001), which approved officers’ reasonable steps to secure a scene to preserve evidence while they awaited a warrant.

B

The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee’s reduced privacy interests upon being taken into police custody. ...

The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. ...
Robinson is the only decision from this Court applying Chimel to a search of the contents of an item found on an arrestee’s person. ... Lower courts applying Robinson and Chimel, however, have approved searches of a variety of personal items carried by an arrestee. See, e.g., United States v. Carrion, 809 F. 2d 1120, 1123, 1128 (5th Cir. 1987) (billfold and address book); United States v. Watson, 669 F. 2d 1374, 1383–1384 (11th Cir. 1982) (wallet); United States v. Lee, 501 F. 2d 89, 892 (D.C. Cir. 1974) (purse).

The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term “cell phone” is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

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

But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not
carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.\(^1\)

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building. See United States v. Jones, 565 U.S. ___, ___ (2012) (Sotomayor, J., concurring) (slip op., at 3) (“GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familiar, political, professional, religious, and sexual associations.”).

Mobile application software on a cell phone, or “apps,” offer a range of tools for managing detailed information about all aspects of a person’s life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase “there’s an app for that” is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user’s life.

In 1926, Learned Hand observed ... that it is “a totally different thing to search a man’s pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.” United States v. Kirschenblatt, 16 F. 2d 202, 203 (2nd Cir. 1926). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in

---

\(^1\) Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.
digital form many sensitive records previously found in the home; it also contains
a broad array of private information never found in a home in any form – unless
the phone is.

To further complicate the scope of the privacy interests at stake, the data a user
views on many modern cell phones may not in fact be stored on the device itself.
Treating a cell phone as a container whose contents may be searched incident to
an arrest is a bit strained as an initial matter. See *New York v. Belton*, 453 U.S. 454,
460, n.4 (1981) (describing a “container” as “any object capable of holding another
object”). But the analogy crumbles entirely when a cell phone is used to access
data located elsewhere, at the tap of a screen. That is what cell phones, with in-
creasing frequency, are designed to do by taking advantage of “cloud computing.”
Cloud computing is the capacity of Internet-connected devices to display data
stored on remote servers rather than on the device itself. Cell phone users often
may not know whether particular information is stored on the device or in the
cloud, and it generally makes little difference. Moreover, the same type of data may
be stored locally on the device for one user and in the cloud for another.

The United States concedes that the search incident to arrest exception may
not be stretched to cover a search of files accessed remotely – that is, a search of
files stored in the cloud. Such a search would be like finding a key in a suspect’s
pocket and arguing that it allowed law enforcement to unlock and search a house.
But officers searching a phone’s data would not typically know whether the infor-
mation they are viewing was stored locally at the time of the arrest or has been
pulled from the cloud.

Although the Government recognizes the problem, its proposed solutions are
unclear. It suggests that officers could disconnect a phone from the network before
searching the device – the very solution whose feasibility it contested with respect
to the threat of remote wiping. Alternatively, the Government proposes that law
enforcement agencies “develop protocols to address” concerns raised by cloud
computing. Probably a good idea, but the Founders did not fight a revolution to
gain the right to government agency protocols. The possibility that a search might
extend well beyond papers and effects in the physical proximity of an arrestee is
yet another reason that the privacy interests here dwarf those in *Robinson*.

Apart from their arguments for a direct extension of *Robinson*, the United States
and California offer various fallback options for permitting warrantless cell phone
searches under certain circumstances. Each of the proposals is flawed and contra-
venes our general preference to provide clear guidance to law enforcement
through categorical rules. ...

The United States first proposes that the *Gant* standard be imported from the
vehicle context, allowing a warrantless search of an arrestee’s cell phone whenever
it is reasonable to believe that the phone contains evidence of the crime of arrest.

At any rate, a *Gant* standard would prove no practical limit at all when it comes
to cell phone searches. In the vehicle context, *Gant* generally protects against
searches for evidence of past crimes. In the cell phone context, however, it is rea-
sonable to expect that incriminating information will be found on a phone regard-
less of when the crime occurred. Similarly, in the vehicle context *Gant* restricts
broad searches resulting from minor crimes such as traffic violations. That would
not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the Gant standard to cell phones would in effect give “police officers unbridled discretion to rummage at will among a person's private effects.”

The United States also proposes a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered. This approach would again impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where.

We also reject the United States’ final suggestion that officers should always be able to search a phone’s call log, as they did in Wurie's case. The Government relies on Smith v. Maryland, 442 U.S. 735 (1979), which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a “search” at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label “my house” in Wurie's case.

Finally, at oral argument California suggested a different limiting principle, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. In Riley’s case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under California's proposal would be able to search a phone for all of those items—a significant diminution of privacy.

In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip? It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact. An analogue test would keep defendants and judges guessing for years to come.

IV

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facili-
tating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow ‘weighed’ against the claims of police efficiency. Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient.

Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment. Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury. In United States v. Chadwick, 433 U.S. 1, 15 (1977), for example, the Court held that the exception for searches incident to arrest did not justify a search of [a 200-pound footlocker], but noted that “if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without opening the luggage.” 433 U.S., at 15 n.9.

In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child’s location on his cell phone. The defendants here recognize – indeed, they stress – that such fact-specific threats may justify a warrantless search of cell phone data. The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case.

*   *   *

Our cases have recognized that the Fourth Amendment was the founding generation’s response to the reviled “general warrants” and “writs of assistance” of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that “[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance.” 10 Works of John Adams 247-248 (C. Adams ed. 1856). According to Adams, Otis’s speech was “the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.” Id., at 248.

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life. The fact that technology now allows an individual to carry such information
in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant. ...

**QUESTIONS**

1. Does *Riley* translate familiar Fourth Amendment principles from the physical world to the digital one? Or does it create new, distinctive principles for computers?

2. A police officer arrests Wiley and finds a phone in his pocket. Just then, a text message from one of Wiley’s co-conspirators arrives, listing the location for a drug buy. The police drive to the location and arrest the co-conspirator. Legal? (Does it matter whether Wiley is using a flip phone or a smartphone that displays incoming texts on the lock screen?) What if the co-conspirator calls Wiley instead, and the police officer picks up the phone and successfully impersonates Wiley long enough to arrange the drug buy?

3. What counts as a “search” of an electronic device? The answer is not always obvious, given that one can interact with it digitally as well as physically. Suppose the police dial what they think is the defendant’s phone number to see whether the phone in his pocket rings. Search? Or what if they use a cell-site simulator (sometimes called a “stingray”): a device that pretends to be a cell tower and records the identifying information and location of cell phones that attempt to connect to it?

4. Dom Toretto was involved in an automobile collision and his badly-damaged car was impounded while he was in the hospital receiving treatment for his injuries. The police suspect that the crash occurred during an illegal high-speed drift-racing competition. They would like to inspect the car’s electronic data recorder, a/k/a “black box,” a small onboard computer which automatically records the car’s speed, engine RPM, steering wheel position, brake status, and other data. Obtaining the data will require inserting a cable into the car’s dashboard, and decoding it will require specialized software available only to mechanics certified by the car’s manufacturer. Do the police need a warrant?

5. Computer searches raise difficult pragmatic questions. The police arrest Bill Maplewood for possession of child pornography. Having read *Riley*, they plan to obtain a warrant to seize his laptop computer and search it for evidence. The laptop’s hard drive also contains his tax records, his emails, and patient records from his psychiatric practice. Which of these can the police examine? How should they carry out the examination? Can they also look for evidence of tax evasion? How long can they retain the laptop? Which of these limits should be detailed in the warrant itself?
Chapter 4: Privacy

UNITED STATES V. WARSHAK
631 F.3d 266 (6th Cir. 2010)

Boggs, Circuit Judge: ...

I. STATEMENT OF THE FACTS

A. Factual Background

In 2001, Steven Warshak (“Warshak”) owned and operated a number of small businesses in the Cincinnati area [including Berkeley Premium Neutraceuticals, Inc. (“Berkeley”).]

In the latter half of 2001, Berkeley launched Enzyte, its flagship product. At the time of its launch, Enzyte was purported to increase the size of a man's erection. The product proved tremendously popular, and business rose sharply. By 2004, demand for Berkeley's products had grown so dramatically that the company employed 1500 people, and the call center remained open throughout the night, taking orders at breakneck speed. Berkeley's line of supplements also expanded, ballooning from approximately four products to around thirteen. By year's end, Berkeley's annual sales topped out at around $250 million, largely on the strength of Enzyte.

1. Advertising

The popularity of Enzyte appears to have been due in large part to Berkeley's aggressive advertising campaigns. The vast majority of the advertising – approximately 98% – was conducted through television spots. Around 2004, network television was saturated with Enzyte advertisements featuring a character called “Smilin' Bob,” whose trademark exaggerated smile was presumably the result of Enzyte's efficacy. The “Smilin' Bob” commercials were rife with innuendo and implied that users of Enzyte would become the envy of the neighborhood.

... [Print and radio commercials] cited a 2001 independent customer study, which purported to show that, over a three-month period, 100 English-speaking men who took Enzyte experienced a 12 to 31% increase in the size of their penises. The 2001 study was also referenced in radio advertisements and appeared on the company's website, as well as in brochures and sales calls. James Teegarden later testified that the survey was bogus. He stated that, prior to the appearance of the advertisements, Warshak instructed him to create a spreadsheet and to fill it with fabricated data. Teegarden testified that he plucked the numbers out of the air and generated the spreadsheet over a twenty-four hour period. ...

2. The Auto-Ship Program

The “life blood” of the business was its auto-ship program, which was instituted in 2001, shortly before Enzyte hit the market. The auto-ship program was a continuity or negative-option program, in which a customer would order a free trial of a product and then continue to receive additional shipments of that product until he opted out. Before each new continuity shipment arrived on the customer's doorstep, a corresponding charge would appear on his credit-card statement. The shipments and charges would continue until the customer decided to withdraw from the program, which required the customer to notify the company.

In the early days of the auto-ship program, customers who ordered products over the phone were not told that they were being enrolled. From August 2001 to at least the end of December 2002, customers were simply added to the program at the time of the initial sale without any indication that they would be on the hook for additional charges. Apparently, products were shipped with literature explaining the program, but no authorization was sought in advance of the ship-
ment. According to Teegarden, Warshak explained that the auto-ship program was never mentioned because “nobody would sign up.” If nobody signed up, “you couldn’t make revenue.”

This policy resulted in a substantial volume of complaints, both to Berkeley and to outside organizations. In October 2002, the Better Business Bureau (“BBB”) contacted Berkeley and indicated that more than 1,500 customers had called to voice their consternation. Because of the complaints, Berkeley’s sales scripts and website began to include some language disclosing the auto-ship program. ...

However, as a number of Berkeley insiders testified, the compulsory disclosure language was not always read, and it was designed not to work. Shelley Kinmon testified that the disclosure of the continuity shipments was only made after the customer had placed his order. In other words, the sales representative had already taken the customer’s credit-card information when auto-ship was mentioned. Also, the disclosures were deliberately made with haste, and they were placed after unrelated language that was intended to divert or deaden the customer’s attention. In the case of Enzyte, sales reps were instructed to lead into the disclosure language by stating that “the product is not a contraceptive nor will it prevent or treat any sexually transmitted disease.” According to Teegarden, the thinking was that, “if we started off with a statement about a contraceptive, something other than what it was, that people wouldn’t really listen to what we were disclosing to them.”

Moreover, disclosure of the auto-ship program was sometimes irrelevant. For example, in November 2003, Berkeley hired a company called West to handle “sales calls that were from . . . Avlimil or Enzyte advertisements.” During the calls, West’s representatives asked customers if they wanted to be enrolled in the auto-ship program, and over 80% of customers declined. When Warshak learned what was happening, he issued instructions to “take those customers, even if they decline[d], even if they said no to the Auto-Ship program, go ahead and put them on the Auto-Ship program.” A subsequent email between Berkeley employees indicated that “all [West] customers, whether they know it or not, are going on [auto-ship].” As a result, numerous telephone orders resulted in unauthorized continuity shipments. ...

[Warshak and Berkeley also systematically misled the banks who processed Berkeley’s credit-card payments. Many customers would dispute Berkeley charges with their credit card companies, resulting in “chargebacks” in which Berkeley was required to issue them refunds. Since many banks and credit-card processors will not do business with merchants who have too many chargebacks, Berkeley lied to banks about its chargeback history and engaged in fake transactions solely to lower its chargeback ratio.]

B. Procedural History
In September 2006, a grand jury sitting in the Southern District of Ohio returned a 112-count indictment charging Warshak ... and several others with various crimes related to Berkeley’s business. Warshak was charged with conspiracy to commit mail, wire, and bank fraud (Count 1); mail fraud (Counts 2-13); making false statements to banks (Counts 14, 16–22, 24–26, 28); bank fraud (Counts 15, 23, 27); conspiracy to commit and attempt to commit access-device fraud (Count 29); conspiracy to commit money laundering (Count 34); money laundering (Counts 32–98, 102–106, 108); conspiracy to commit misbranding (Count 109); misbranding (Count 110); and, lastly, conspiracy to obstruct a Federal Trade Commission (“FTC”) proceeding (Count 112). ...
Before trial, numerous motions were filed. First, Warshak moved to exclude thousands of emails that the government obtained from his Internet Service Providers. That motion was denied...

Over fifteen months later, in January 2008, the case proceeded to trial. Approximately six weeks later, the trial ended and the defendants were convicted of the majority of the charges...

On August 27, 2008, the defendants were sentenced. Warshak received a sentence of 25 years of imprisonment. He was also ordered to pay a fine of $93,000 and a special assessment of $9,300. In addition, he was ordered to surrender $459,540,000 in proceeds-money-judgment forfeiture and $44,876,781.68 in money-laundering-judgment forfeiture...

II. Analysis

A. The Search & Seizure of Warshak’s Emails

Warshak argues that the government’s warrantless, ex parte seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment’s prohibition on unreasonable searches and seizures. The government counters that, even if government agents violated the Fourth Amendment in obtaining the emails, they relied in good faith on the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701 et seq., a statute that allows the government to obtain certain electronic communications without procuring a warrant. The government also argues that any hypothetical Fourth Amendment violation was harmless. We find that the government did violate Warshak’s Fourth Amendment rights by compelling his Internet Service Provider (“ISP”) to turn over the contents of his emails...

1. The Stored Communications Act


2. Factual Background

Email was a critical form of communication among Berkeley personnel. As a consequence, Warshak had a number of email accounts with various ISPs, including an account with NuVox Communications. In October 2004, the government formally requested that NuVox prospectively preserve the contents of any emails to or from Warshak’s email account. ... NuVox acceded to the government’s request and began preserving copies of Warshak’s incoming and outgoing emails – copies that would not have existed absent the prospective preservation request. Per the government’s instructions, Warshak was not informed that his messages were being archived.

In January 2005, the government obtained a subpoena under § 2703(b) and compelled NuVox to turn over the emails that it had begun preserving the previous year. In May 2005, the government served NuVox with an ex parte court order under § 2703(d) that required NuVox to surrender any additional email messages in Warshak’s account. In all, the government compelled NuVox to reveal the contents of approximately 27,000 emails. Warshak did not receive notice of either the subpoena or the order until May 2006.

3. The Fourth Amendment

The Fourth Amendment provides that “[t]he 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. . . .” U.S. Const. amend. IV. The fundamental purpose of the Fourth Amendment “is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.” Camara v. Mun. Ct., 387 U.S. 523, 528 (1967)...


Turning first to the subjective component of the test, we find that Warshak plainly manifested an expectation that his emails would be shielded from outside scrutiny. As he notes in his brief, his “entire business and personal life was contained within the . . . emails seized.” Appellant’s Br. at 39–40. Given the often sensitive and sometimes damning substance of his emails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view. Therefore, we conclude that Warshak had a subjective expectation of privacy in the contents of his emails.

The next question is whether society is prepared to recognize that expectation as reasonable. This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, “account” is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner’s life. By obtaining access to someone’s email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber’s emails without triggering the machinery of the Fourth Amendment.

In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.

With those principles in mind, we begin our analysis by considering the manner in which the Fourth Amendment protects traditional forms of communication. In Katz, the Supreme Court was asked to determine how the Fourth Amendment applied in the context of the telephone. There, government agents had affixed an electronic listening device to the exterior of a public phone booth, and had used the device to intercept and record several phone conversations. The Supreme
Court held that this constituted a search under the Fourth Amendment, notwithstanding the fact that the telephone company had the capacity to monitor and record the calls. In the eyes of the Court, the caller was "surely entitled to assume that the words he uttered into the mouthpiece would not be broadcast to the world." *Katz*, 389 U.S. at 352. The Court's holding in *Katz* has since come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means.

Letters receive similar protection. While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private. See *Katz*, 389 U.S. at 351 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. ... Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification." [*City of Ontario v.* Quon], 130 S. Ct. at 2630. It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment must recognize and protect nascent ones that arise. See *Warshak I*, 490 F.3d at 473 ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.").

If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call – unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.

In *Warshak I*, the government argued that this conclusion was improper, pointing to the fact that NuVox contractually reserved the right to access Warshak's emails for certain purposes. While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of
privacy in the contents of an email account, ... we doubt that will be the case in most situations, and it is certainly not the case here.

As an initial matter, it must be observed that the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. See *Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting). Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy.

Nor is the right of access. As the Electronic Frontier Foundation points out in its *amicus* brief, at the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to “protect themselves and their properties against the improper and illegal use of their facilities.” *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967). In this case, the NuVox subscriber agreement tracks that language, indicating that “NuVox may access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service.” Acceptable Use Policy, available at http://business.windstream.com/Legal/acceptableUse.htm (last visited Aug. 12, 2010). Thus, under *Katz*, the degree of access granted to NuVox does not diminish the reasonableness of Warshak’s trust in the privacy of his emails.16

Our conclusion finds additional support in the application of Fourth Amendment doctrine to rented space. Hotel guests, for example, have a reasonable expectation of privacy in their rooms. See *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997). This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. See *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009). That expectation persists, regardless of the incursions of handymen to fix leaky faucets. Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question.

Again, however, we are unwilling to hold that a subscriber agreement will never be broad enough to snuff out a reasonable expectation of privacy. As the panel noted in *Warshak I*, if the ISP expresses an intention to “audit, inspect, and monitor” its subscriber’s emails, that might be enough to render an expectation of privacy unreasonable. See 490 F.3d at 472-73 (quoting *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000)). But where, as here, there is no such statement, the ISP’s “control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy.” *Id.* at 473.

We recognize that our conclusion may be attacked in light of the Supreme Court’s decision in *United States v. Miller*, 425 U.S. 435 (1976). In *Miller*, the Supreme Court held that a bank depositor does not have a reasonable expectation of privacy in the contents of bank records, checks, and deposit slips. *Id.* at 442. The Court’s holding in *Miller* was based on the fact that bank documents, “includ-

---

16 We note that the access granted to NuVox was also temporally limited, as Warshak’s email account was configured to delete his emails from NuVox’s servers as soon as he opened them on his personal computer.
ing financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” *Ibid.* The Court noted,

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

*Ibid.* at 443 (citations omitted).

But *Miller* is distinguishable. First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of “confidential communications” at issue here. See *ibid.* Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use “in the ordinary course of business.” *Ibid.* By contrast, Warshak received his emails through NuVox. NuVox was an intermediary, not the intended recipient of the emails. See Bellia & Freiwald, *Stored E-Mail*, 2008 U. Chi. Legal F. at 165 (“[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer’s interests.”). Thus, *Miller* is not controlling.

Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails “that are stored with, or sent or received through, a commercial ISP.” *Warshak I*, 490 F.3d at 473. ... The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak’s emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.

**QUESTIONS**

1. Presumably, Warshak’s computer also contained copies of his emails. Why didn’t the government simply seize the computer and search through the emails on it?

2. In the actual case, the government obtained a subpoena under § 2703 of the Stored Communications Act (SCA). The SCA is discussed in more detail in the Wiretapping section, but the relevant standard is that the government must present the court with “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.” Is this an easier standard to meet than probable cause, or harder? Why doesn’t the government’s compliance with the terms of the SCA dispose of this case? (*Hint:* these two questions are related.)

3. If you send an email to a friend describing your plans to assassinate the mayor of Metropolis, does the Fourth Amendment prohibit your friend from turning over the email to the Metropolis Police Department? If you send sexually explicit instant messages to “WetRiffs13,” who turns out to be a 35-
year-old FBI agent, have your Fourth Amendment rights been violated? Are these hypotheticals on point with Warshak? Or consider United States v. Morel, 2017 DNH 072, 2017 WL 1376363 (D.N.H. Apr. 14, 2017), in which the defendant uploaded several images containing child pornography to the file-sharing site Imgur, where anyone with the URL could view them. This, the court held, was inconsistent with “taking affirmative steps to protect the information” — even without further proof that the defendant had actually shared the URL with anyone. Is this result consistent with Warshak?

4. Warshak explains that an email is more like a letter or a phone call (Katz) than a bank record (Miller). Is the argument persuasive? How effective is the process of reasoning by analogy when it comes to new technologies? Consider another hypothetical. Google’s Chrome web browser has a “sync” feature that will transfer your bookmarks from one computer to another. To make it work, your copy of Chrome on the first computer needs to transmit the list of bookmarks to Google’s servers, from which your second computer can then download it. After Warshak, would the government need a search warrant to get the list of your bookmarks from Google?

5. If you were reading the quoted language from NuVox’s subscriber agreement, when, if ever, would you expect a human employee of NuVox to read your emails? Until 2017, Gmail used computers to automatically scan the contents of users’ emails and display ads based on the topics they’re discussing. After Warshak, did Gmail users have an expectation of privacy in their emails? What about people who sent email to Gmail users?

6. Other courts have been more willing to hold that terms of service can destroy an expectation of privacy. For example, in Holmes v. Petrovich Development Co., 191 Cal. App. 4th 1047 (Ct. App. 2011), the court held that a company’s acceptable use policy (which stated that work computers were not to be used for personal purposes and that all computer use could be monitored) meant that an employee waived the attorney-client privilege by using her work computer to email her lawyer. Can Holmes be reconciled with Warshak?

UNITED STATES V. APPLE MACPRO COMPUTER
851 F.3d 238 (3d Cir. 2017)

Vanaskie, Circuit Judge: ...

The District Court found Appellant John Doe in civil contempt for refusing to comply with an order issued pursuant to the All Writs Act, 28 U.S.C. § 1651, which required him to produce several seized devices in a fully unencrypted state. Doe contends that ... the order itself violates his Fifth Amendment privilege against self-incrimination.

I.

During an investigation into Doe’s access to child pornography over the internet, the Delaware County Criminal Investigations Unit executed a valid search warrant at Doe’s residence. During the search, officers seized an Apple iPhone 5S and an Apple Mac Pro Computer with two attached Western Digital External Hard Drives, all of which had been protected with encryption software. Police subsequently seized a password-protected Apple iPhone 6 Plus as well.

Agents from the Department of Homeland Security then applied for a federal search warrant to examine the seized devices. Doe voluntarily provided the pass-
word for the Apple iPhone 5S, but refused to provide the passwords to decrypt the Apple Mac Pro computer or the external hard drives. Despite Doe's refusal, forensic analysts discovered the password to decrypt the Mac Pro Computer, but could not decrypt the external hard drives. Forensic examination of the Mac Pro revealed an image of a pubescent girl in a sexually provocative position and logs showing that the Mac Pro had been used to visit sites with titles common in child exploitation, such as “toddler_cp,” “lolilcam,” “tor-childporn,” and “pthc.” The forensic examination also disclosed that Doe had downloaded thousands of files known by their “hash” values to be child pornography. The files, however, were not on the Mac Pro, but instead had been stored on the encrypted external hard drives. Accordingly, the files themselves could not be accessed.

As part of their investigation, the Delaware County law enforcement officers also interviewed Doe’s sister, who had lived with Doe during 2015. She related that Doe had shown her hundreds of images of child pornography on the encrypted external hard drives. She told the investigators that the external hard drives included “videos of children who were nude and engaged in sex acts with other children.” Doe provided the password to access the iPhone 6 Plus, but did not grant access to an application on the phone which contained additional encrypted information. Forensic analysts concluded that the phone’s encrypted database contained approximately 2,015 image and video files.

On August 3, 2015, upon application of the Government, a Magistrate Judge issued an order pursuant to the All Writs Act requiring Doe to produce his iPhone 6 Plus, his Mac Pro computer, and his two attached external hard drives in a fully unencrypted state (the “Decryption Order”). Doe produced the Apple iPhone 6 Plus, including the files on the secret application, in a fully unencrypted state by entering three separate passwords on the device. The phone contained adult pornography, a video of Doe’s four-year-old niece in which she was wearing only her underwear, and approximately twenty photographs which focused on the genitals of Doe’s six-year-old niece. Doe, however, stated that he could not remember the passwords necessary to decrypt the hard drives and entered several incorrect passwords during the forensic examination. The Government remains unable to view the decrypted content of the hard drives without his assistance.

Following the forensic examination, the Magistrate Judge granted the Government’s Motion for Order to Show Cause Why Doe Should Not Be Held in Contempt, finding that Doe willfully disobeyed and resisted the Decryption Order. Based on the evidence presented at the hearing, the Magistrate Judge found that Doe remembered the passwords needed to decrypt the hard drives but chose not to reveal them because of the devices’ contents.

III...

B...

Doe also contends that the Decryption Order violates his Fifth Amendment privilege against self-incrimination...

The Fifth Amendment states that “[n]o person ... shall be compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. The Fifth Amendment, however, “does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is incriminating.” Fisher v. United States, 425 U.S. 391, 408 (1976). To be testimonial, a communication must
either “explicitly or implicitly ... relate a factual assertion or disclose information.”


The Supreme Court has recognized that in some instances, the production of evidence can implicate the Fifth Amendment. In Fisher, the Court stated that “[t]he act of producing evidence in response to a subpoena ... has communicative aspects of its own, wholly aside from the contents of the papers produced.” 425 U.S. at 410. The Court reasoned that compliance with a request for evidence may “tacitly concede[ ] the existence of the documents demanded and their possession and control by the [defendant].” Id. By “producing documents, one acknowledges that the documents exist, admits that the documents are in one’s custody, and concedes that the documents are those that the [Government] requests.” United States v. Chabot, 793 F.3d 338, 342 (3d Cir.). When the production of evidence does concede the existence, custody, and authenticity of that evidence, the Fifth Amendment privilege against self-incrimination applies because that production constitutes compelled testimony.

In Fisher, however, the Court also articulated the “foregone conclusion” rule, which acts as an exception to the otherwise applicable act-of-production doctrine. Under this rule, the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a “foregone conclusion” that “adds little or nothing to the sum total of the Government’s information.” For the rule to apply, the Government must be able to “describe with reasonable particularity” the documents or evidence it seeks to compel. U.S. v. Hubbell, 530 U.S. 27, 30 (2000).

Although we have not confronted the Fifth Amendment implications of compelled decryption, the Eleventh Circuit has addressed the issue and found that the privilege against self-incrimination should apply. In that case, a suspect appealed a judgment of contempt entered after he refused to produce the unencrypted contents of his laptop and hard drives. In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1337 (11th Cir. 2012). The court found that “(1) [the suspect’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.” Id. at 1346. The court reached this decision after noting that the Government did not show whether any files existed on the hard drives and could not show with any reasonable particularity that the suspect could access the encrypted portions of the drives. Although the court did not require the Government to identify exactly the documents it sought, it did require that, at the very least, the Government be able to demonstrate some knowledge that files do exist on the encrypted devices.

Despite Doe’s argument to the contrary, the Eleventh Circuit’s reasoning in In re Grand Jury Subpoena does not compel a similar result here. The Magistrate Judge found that, though the Fifth Amendment may be implicated by Doe’s decryption of the devices, any testimonial aspects of that production were a foregone conclusion. According to the Magistrate Judge, the affidavit supporting the application for the search warrant established that (1) the Government had custody of the devices; (2) prior to the seizure, Doe possessed, accessed, and owned all devices; and (3) there are images on the electronic devices that constitute child pornography. ...

Unlike In re Grand Jury Subpoena, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe
can access them. The affidavit supporting the search warrant states that an investigation led to the identification of Doe as a user of an internet file sharing network that was used to access child pornography. When executing a search of Doe's residence, forensic analysts found the encrypted devices, and Doe does not dispute their existence or his ownership of them. Once the analysts accessed Doe's Mac Pro Computer, they found one image depicting a pubescent girl in a sexually suggestive position and logs that suggested the user had visited groups with titles common in child exploitation. Doe's sister then reported that she had witnessed Doe unlock his Mac Pro while connected to the hard drives to show her hundreds of pictures and videos of child pornography. Forensic analysts also found an additional 2,015 videos and photographs in an encrypted application on Doe's phone, which Doe had opened for the police by entering a password. Based on these facts, the Magistrate Judge found that, for the purposes of the Fifth Amendment, any testimonial component of the production of decrypted devices added little or nothing to the information already obtained by the Government. The Magistrate Judge determined that any testimonial component would be a foregone conclusion. The Magistrate Judge did not commit a clear or obvious error in his application of the foregone conclusion doctrine. In this regard, the Magistrate Judge rested his decision rejecting the Fifth Amendment challenge on factual findings that are amply supported by the record. Accordingly, Doe's challenges to the Decryption Order and Quashal Denial fail.

So, too, does Doe's challenge to the contempt order. At the hearing on the contempt motion, Doe maintained that he could not remember the passwords to decrypt the hard drives. In a civil contempt proceeding, when a defendant raises a challenge of impossibility of compliance, the defendant bears the burden of production. At the contempt hearing, the Government presented several witnesses to support its prima facie case of contempt. Doe's sister testified to the fact that, while in her presence, Doe accessed child pornography files on his Mac Pro computer by means of entering passwords from memory. Further, a detective who executed the original search warrant stated that Doe did not provide his password at the time because he wanted to prevent the police from accessing his computer. Doe never asserted an inability to remember the passwords at that time. Doe presented no evidence to explain his failure to comply or to challenge the evidence brought by the Government. The District Court thus found Doe in contempt and ordered he be held in custody until he complies with the Decryption Order. The

7. It is important to note that we are not concluding that the Government’s knowledge of the content of the devices is necessarily the correct focus of the “foregone conclusion” inquiry in the context of a compelled decryption order. Instead, a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is “I, John Doe, know the password for these devices.” Based upon the testimony presented at the contempt proceeding, that fact is a foregone conclusion. However, because our review is limited to plain error, and no plain error was committed by the District Court in finding that the Government established that the contents of the encrypted hard drives are known to it, we need not decide here that the inquiry can be limited to the question of whether Doe's knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine.
District Court did not abuse its discretion in finding Doe to be in contempt of the Decryption Order.

**QUESTIONS**

1. Is the password to a computer like the key to a locked box? The combination to a safe? Would it be “testimonial” to require the production of a key or a combination?

2. Do you see how something can be testimonial and still also be a foregone conclusion?

3. When Al Bertillon is arrested for conspiracy to distribute a controlled substance, the police seize an iPhone from his backpack, which is secured not with a passcode but with a fingerprint lock. Can the police compel him to put his thumb on the phone’s fingerprint sensor?

4. The government can also try to obtain passwords surreptitiously. This works surprisingly often. In *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001), the FBI broke into the defendant’s office and installed a “key logger” on his computer keyboard that recorded his keystrokes. The FBI thereby obtained the password he used to encrypt his files, which contained evidence of gambling and loansharking. Do you see any Fourth Amendment issues with this procedure? If so, how would you carry it out so that the resulting evidence would be admissible in court?

**COFFEESHOP PROBLEM**

Officer Augusta Zenobia from the King County Sheriff’s Office is ordering an americano at a Tully’s Coffee Shop in Seattle when she notices that one of the other patrons has left an unattended laptop sitting on a table. It has shifted over into the screensaver, which appears to be pulling random pictures from the computer’s hard drive. Some of them show people who appear to be naked and underage.

A few seconds later, a man emerges from the men’s room and walks towards the table with the laptop. He makes brief eye contact with Officer Zenobia, then looks back to the laptop, which has just flashed up another photo of someone without clothes on. He runs for the computer and slams it shut. Officer Zenobia is a few steps behind; she orders him away from the computer and places him under arrest. He turns out to be one Lucius Aurelian; he has a clean criminal record. The computer, along with the other items he had on his person (a wallet, keys, a laptop bag, some papers for work), are currently sitting in the evidence locker at the police station.

You work in the King County Prosecuting Attorney’s office, and you have been assigned the case. Officer Zenobia is willing to testify that the images she saw were clearly child pornography. How good a case will you be able to build? What should the next steps in the investigation be?

**B. Wiretapping**

The Constitution is hardly the only source of communications privacy law. A variety of federal and state statutes also regulate the use and disclosure of information stored in computers or transmitted on networks. This section examines three principal federal statutes on point: the Wiretap Act (codified at 18 U.S.C. §§ 2510–
Chapter 4: Privacy

2522), the Stored Communications Act (the SCA, codified at 18 U.S.C. §§ 2701–2712) and the Pen Register and Trap and Trace statute (codified at 18 U.S.C. §§ 3121–27). All three were heavily amended by the Electronic Communications Privacy Act of 1986, or ECPA, which is sometimes used to refer to the field as a whole and sometimes used as a synonym for the SCA. These statutes have two interlocking roles:

- To protect individuals from having their private communications seen by other private parties.
- To regulate the process by which the government acquires private communications during investigations.

Unfortunately for statutory clarity, these two roles are utterly intermingled in the federal communications privacy statutes. All three take the form of a general prohibition on unauthorized access, together with exceptions for private and governmental access under certain circumstances. Figuring out what law applies to a given situation is often a matter of extensive back-and-forth cross-referencing. As you read through the statutes, keep in mind the private/governmental distinction and, also, whether the communications are being intercepted while in transit (“prospectively”), or retrieved after the fact (“retrospectively”). A third crucial distinction, familiar from the Fourth Amendment materials, is between the “contents” of a communication and other “non-content” information about it.

**WIRETAP ACT**

**Title 18, United States Code**

§ 2510 - Definitions

(1) “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication; ...

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. ...

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; ...

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include –

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds; ...

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; ...

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications; ...

(17) “electronic storage” means –

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; ...

§ 2511 – Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who –

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; ...

shall be punished as provided in subsection (4). ...

(2) ...

(a) ...

(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. ...

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose
of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State. ...

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person –

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public ...

§ 2515 – Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2518 – Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant’s authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued ...

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; ...

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications ... if the judge determines on the basis of the facts submitted by the applicant that –

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (II), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense,
or are leased to, listed in the name of, or commonly used by such person. ...

**QUESTIONS**

1. The core prohibition of the Wiretap Act is in § 2511(1), which must be read together with the relevant definitions in § 2510. Which of the following are illegal under the Wiretap Act?
   - Planting a hidden digital voice recorder in a meeting room used by corporate executives?
   - Standing on a toilet seat to overhear a conversation between two other people in the bathroom without being noticed?
   - Setting up the laptop computers issued to middle-school students to take a picture using the built-in camera every thirty seconds?
   - Using a radio receiver to listen in on cordless phone conversations from nearby houses (but not saving a copy of the audio).

2. The Wiretap Act contains many exceptions. The most important of these is set forth in § 2518, which outlines a procedure for submitting an application to a court to install a wiretap. Who is allowed to make the application? What evidence do they need to provide? Is it easier to obtain a search warrant or a wiretap order? Can private parties obtain judicial authorization for one?

3. The “provider exception” in § 2511(2)(a) is also important. To whom does it apply, and how broad is it? Is it a Wiretap Act violation for Gmail to deliver email to users? To display ads next to the emails based on their contents? For Google employees to randomly inspect a sample of emails to see whether the ad displays are working?

4. States have their own wiretapping laws. New York, for example, prohibits “recording of a telephonic ... communication by a person other than a sender or a receiver thereof.” N.Y. Penal L. §§ 250.00, 250.05. In California, it is illegal to record a “confidential communication” without the “consent of all parties.” Cal. Pen. Code § 632(a). If Linda, in California, tape-records her phone calls with Monica, in New York, and Monica doesn’t know about it, is this a violation of New York Law? California Law?

**O’BRIEN V. O’BRIEN**

899 So. 2d 1133 (Fla. Dist. Ct. App. 5th 2005)

_Sawaya, Chief Judge:_

Emanating from a rather contentious divorce proceeding is an issue we must resolve regarding application of certain provisions of the Security of Communications Act (the Act) found in Chapter 934, Florida Statutes (2003). Specifically, we must determine whether the trial court properly concluded that pursuant to section 934.03(1), Florida Statutes (2003), certain communications were inadmissible because they were illegally intercepted by the Wife who, unbeknownst to the Husband, had installed a spyware program on a computer used by the Husband that copied and stored electronic communications between the Husband and another woman.

When marital discord erupted between the Husband and the Wife, the Wife secretly installed a spyware program called Spector on the Husband’s computer. It is undisputed that the Husband engaged in private on-line chats with another
woman while playing Yahoo Dominoes on his computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of these snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. When the Husband discovered the Wife’s clandestine attempt to monitor and record his conversations with his Dominoes partner, the Husband uninstalled the Spector software and filed a Motion for Temporary Injunction, which was subsequently granted, to prevent the Wife from disclosing the communications. …

... The Wife argues that the electronic communications do not fall under the umbra [sic] of the Act because these communications were retrieved from storage and, therefore, are not “intercepted communications” as defined by the Act. In opposition, the Husband contends that the Spector spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, are intercepts illegally obtained under the Act.

The trial court found that the electronic communications were illegally obtained in violation of section 934.03(1)(a)(e), and so we begin our analysis with the pertinent provisions of that statute, which subjects any person to criminal penalties who engages in the following activities:

(a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication; ...  

... It is beyond doubt that what the trial court excluded from evidence are “electronic communications.” The core of the issue lies in whether the electronic communications were intercepted. The term “intercept” is defined by the Act as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” § 934.02(3), Fla. Stat. (2003). We discern that there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated. It is here that we tread upon new ground. Because we have found no precedent rendered by the Florida courts that considers this distinction, and in light of the fact that the Act was modeled after the Federal Wiretap Act, we advert to decisions by the federal courts that have addressed this issue for guidance.

The federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. United States v. Steiger, 318 F.3d 1039 (11th Cir.), ... [T]he particular facts and circumstances of the instant case reveal that the electronic communications were intercepted contemporaneously with transmission.

The Spector spyware program that the Wife surreptitiously installed on the computer used by the Husband intercepted and copied the electronic communications as they were transmitted. We believe that particular method constitutes interception within the meaning of the Florida Act, and the decision in Steiger supports this conclusion. In Steiger, an individual was able to hack into the defendant’s computer via a Trojan horse virus that allowed the hacker access to pornographic materials stored on the hard drive. The hacker was successful in transferring the pornographic material from that computer to the hacker’s computer. The
court held that because the Trojan horse virus simply copied information that had previously been stored on the computer's hard drive, the capture of the electronic communication was not an interception within the meaning of the Federal Wiretap Act. The court did indicate, however, that interception could occur if the virus or software intercepted the communication as it was being transmitted and copied it. The court stated:

[T]here is only a narrow window during which an E-mail interception may occur – the seconds or milliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

Steiger, 318 F.3d at 1050 (quoting Jarrod J. White, E-Mail@Work.com: Employer Monitoring of Employee E-Mail, 48 Ala. L.Rev. 1079, 1083 (1997)). Hence, a valid distinction exists between a spyware program similar to that in Steiger, which simply breaks into a computer and retrieves information already stored on the hard drive, and a spyware program similar to the one installed by the Wife in the instant case, which copies the communication as it is transmitted and routes the copy to a storage file in the computer.

The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic storage. We conclude that because the spyware installed by the Wife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act.

We must next determine whether the improperly intercepted electronic communications may be excluded from evidence under the Act. The exclusionary provisions of the Act are found in section 934.06, Florida Statutes (2003), which provides that “[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence. . . .” Conspicuously absent from the provisions of this statute is any reference to electronic communications. The federal courts, which interpreted an identical statute contained in the Federal Wiretap Act, have held that because provision is not made for exclusion of intercepted electronic communications, Congress intended that such communications not be excluded under the Federal Wiretap Act. See Steiger. We agree with this reasoning and conclude that the intercepted electronic communications in the instant case are not excludable under the Act. But this does not end the inquiry.

Although not specifically excludable under the Act, it is illegal and punishable as a crime under the Act to intercept electronic communications. § 934.03, Fla. Stat. (2003). The trial court found that the electronic communications were illegally intercepted in violation of the Act and ordered that they not be admitted in evidence. Generally, the admission of evidence is a matter within the sound discretion of the trial court. Because the evidence was illegally obtained, we conclude that the trial court did not abuse its discretion in refusing to admit it.
QUESTIONS

1. *O’Brien* is a civil suit between two private parties. How does the Florida criminal wiretapping statute enter into it?

2. The Wiretap Act includes a prohibition on the manufacture or sale in interstate commerce of “any electronic, mechanical, or other device ... primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.” 18 U.S.C. § 2512(1)(a). What does this prohibition add to the prohibition on wiretapping itself? Is Spector such a device?

3. Email works by successively copying the entire message from one computer to another until it reaches its destination. Once it has been copied to the final computer, a program called a “mail delivery agent” (MDA) makes one last copy, adding the email to a particular user’s inbox file, which her own email program can then read. Consider:

   Umberto Causabon, a rare-book dealer, runs a small email service that gives accounts to other rare book dealers. He configures the MDA on his server to scan each incoming email. If the email contains the word “book,” the MDA saves a copy of the email in Causabon’s account as well as copying it to the user’s inbox file. Neither Causabon nor any other person has ever examined the copies made this way.

Has Causabon violated the Wiretap Act?

STORED COMMUNICATIONS ACT

Title 18, United States Code

§ 2701 – *Unlawful access to stored communications*

(a) **Offense.** – Except as provided in subsection (c) of this section whoever –

   (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

   (2) intentionally exceeds an authorization to access that facility;

   and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section. ...

(c) **Exceptions.** – Subsection (a) of this section does not apply with respect to conduct authorized –

   (1) by the person or entity providing a wire or electronic communications service;

   (2) by a user of that service with respect to a communication of or intended for that user; or

   (3) in section 2703, 2704 or 2518 of this title.

§ 2702 – *Voluntary disclosure of customer communications or records*

(a) **Prohibitions.** – Except as provided in subsection (b) or (c) –

   (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; ...
(3) a provider of ... electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) ...) to any governmental entity.

(b) **Exceptions for disclosure of communications.** – A provider described in subsection (a) may divulge the contents of a communication –

1. to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
2. as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title;
3. with the lawful consent of the originator or an addressee or intended recipient of such communication ...
4. to a person employed or authorized or whose facilities are used to forward such communication to its destination;
5. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; ...
6. to a law enforcement agency –
    (A) if the contents –
        (i) were inadvertently obtained by the service provider; and
        (ii) appear to pertain to the commission of a crime; or
7. to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) **Exceptions for Disclosure of Customer Records.** – A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service... –

1. as otherwise authorized in section 2703;
2. with the lawful consent of the customer or subscriber;
3. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
4. to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; ...
5. to any person other than a governmental entity.

§ 2703 – Required disclosure of customer communications or records

(a) **Contents of Wire or Electronic Communications in Electronic Storage.** – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the dis-
closure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) **Contents of Wire or Electronic Communications** [stored with an electronic communication service]. –

(1) A governmental entity may require a provider of [electronic communication service] to disclose the contents of any wire or electronic communication [held in electronic storage for more than 180 days] –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title. ... 

(c) **Records Concerning Electronic Communication Service.** –

(1) A governmental entity may require a provider of electronic communication service ... to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity –

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; ... or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service ... shall disclose to a governmental entity the –

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number)

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (I).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) **Requirements for Court Order.** – A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) **No Cause of Action Against a Provider Disclosing Information Under This Chapter.** – No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter. ...

**QUESTIONS**

1. What is the difference between the SCA and the Wiretap Act? They have a similar structure – prohibition with exceptions – but different coverage. Explain.

2. Start with the portions of the SCA that govern access to communications themselves. (The provisions that govern access to “subscriber information” are discussed in the next section.) There are actually two of them, in §§ 2701(a) and 2702(a)(1). What is the difference between them? Do these sections prohibit actions by private parties, by the government, or by both? And do these sections make Gmail illegal? After all, doesn’t it “access” stored emails all the time?

3. The SCA’s strong protections for stored communications are subject to a great many exceptions. Read the exceptions in §§ 2701(c) and 2702(b). Which situations do they apply to? For whose benefit were they drafted? Which ones do you think are the most important and most frequently used in practice? Are they broader or narrower than the exceptions under the Wiretap Act?
4. The SCA also includes provisions that allow the police to require the disclosure of stored communications under certain circumstances. Where are they? What showing must the police make? Under what circumstances can the government gain access to stored electronic communications with less than a full search warrant? Can private parties avail themselves of this required disclosure procedure?

5. Refer back to United States v. Warshak, supra. After Warshak, which portions of § 2703 are unconstitutional? What must the government do if it seeks email content held by Yahoo! Mail? How much of a difference is this likely to make in a typical investigation?

6. The SCA does not have a suppression remedy: evidence obtained in violation of it can still be used in court. Would a suppression remedy be a good idea?

7. The SCA’s implications for criminal prosecutions are obvious. What does it do to the discovery process in civil litigation? Suppose you represent the defendant in a personal-injury suit and you suspect that the plaintiff’s emails to a friend discussing a recent vacation will demonstrate that her injuries are less severe than she claims. What will happen if you send a subpoena to her email provider?

**EHLING V. MONMOUTH-OCEAN HOSPITAL SERVICE CORP.**

872 F. Supp. 2d 369 (D.N.J. 2012)

Martini, District Judge:

Plaintiff Deborah Ehling filed this action against Monmouth–Ocean Hospital Service Corp. (“MONOC”), Vincent Robbins, and Stacy Quagliana (collectively “Defendants”). This matter comes before the Court on Defendants’ motion for summary judgment ...

I. Background

Plaintiff Deborah Ehling is a registered nurse and paramedic. Defendant MONOC is a non-profit hospital service corporation dedicated to providing emergency medical services to the citizens of the State of New Jersey. Defendant Vincent Robbins is the President and CEO of MONOC. Defendant Stacy Quagliana is the Executive Director of Administration at MONOC.

Plaintiff was hired by MONOC in 2004 as a registered nurse and paramedic ...

A. The Facebook Incident ...

During the 2008–2009 timeframe, Plaintiff maintained a Facebook account and had approximately 300 Facebook friends. Plaintiff selected privacy settings for her account that limited access to her Facebook wall to only her Facebook friends. Plaintiff did not add any MONOC managers as Facebook friends. However, Plaintiff added many of her MONOC coworkers as friends, including a paramedic named Tim Ronco. Plaintiff posted on Ronco’s Facebook wall, and Ronco had access to Plaintiff’s Facebook wall. Unbeknownst to Plaintiff, Ronco was taking screenshots of Plaintiff’s Facebook wall and printing them or emailing them to MONOC manager Andrew Caruso. Ronco and Caruso became friends while working together at a previous job, but Ronco never worked in Caruso’s division at MONOC. The evidence reflects that Ronco independently came up with the idea to provide Plaintiff’s Facebook posts to Caruso. Caruso never asked Ronco for any information about Plaintiff, and never requested that Ronco keep him apprised of
Plaintiff’s Facebook activity. In fact, Caruso was surprised that Ronco showed him Plaintiff’s Facebook posts. Caruso never had the password to Ronco’s Facebook account, Plaintiff’s Facebook account, or any other employee’s Facebook account. Once Caruso received copies of Plaintiff’s Facebook posts, he passed them on to Quagliana, MONOC’s Executive Director of Administration.

On June 8, 2009, Plaintiff posted the following statement to her Facebook wall:

An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards .... go to target practice.

After MONOC management was alerted to the post, Plaintiff was temporarily suspended with pay, and received a memo stating that MONOC management was concerned that Plaintiff’s comment reflected a “deliberate disregard for patient safety.” ...

[Ehling accumulated numerous warning notices and disciplinary points for “unauthorized late swipe-outs, excessive call-outs, failing to have sufficient paid time off to cover hours not worked, refusing 9–1–1 calls, and failing to submit the proper documentation for her ambulance shifts.” She was issued a notice of termination on July 22, 2011, but it was never enforced. Instead, Ehling’s employment was terminated on February 7, 2012, following a dispute about her eligibility for a medical leave of absence. She filed a nine-count complaint, and the defendants moved for summary judgment.]

III. DISCUSSION

A. Count 1: Federal Stored Communications Act

In Count 1, Plaintiff asserts a claim for violation of the Federal Stored Communications Act (or “SCA”), 18 U.S.C. §§ 2701–11. Plaintiff argues that Defendants violated the SCA by improperly accessing her Facebook wall post about the museum shooting. Plaintiff argues that her Facebook wall posts are covered by the SCA because she selected privacy settings limiting access to her Facebook page to her Facebook friends. Defendants disagree and argue that, even if the SCA applies, the facts in this case fall under one of the SCA’s statutory exceptions. For the reasons set forth below, the Court finds that non-public Facebook wall posts are covered by the SCA, and that one of the exceptions to the SCA applies. The Court will address each issue in turn.

i. The SCA Covers Non–Public Facebook Wall Posts

The first issue before the Court is whether the SCA applies to Facebook wall posts. ...

Because the SCA was passed in 1986, the statute “is best understood by considering its operation and purpose in light of the technology that existed in 1986.” William Jeremy Robison, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 GEO. L.J. 1195, 1204 (2010). Computer networking was in its infancy in 1986. In the mid–1980s, “personal users [had just begun] subscribing to self-contained networks, such as Prodigy, CompuServe, and America Online.” Id. After connecting to a network via a modem, users could download or send e-mail to other users, access a closed universe of content, and post mes-
messages on electronic bulletin board systems (“BBS’s”). A BBS was “a computer pro-
gram that simulate[d] an actual bulletin board by allowing computer users who
was enacted before the advent of the World Wide Web in 1990 and before the intr-
duction of the web browser in 1994. “Despite the rapid evolution of computer
and networking technology since the SCA’s adoption, its language has remained
surprisingly static.” Id. at 1196. Thus, the “task of adapting the Act’s language to
modern technology has fallen largely upon the courts.” Id.

The SCA provides that whoever “(1) intentionally accesses without authoriza-
tion a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility; and thereby ob-
tains, alters or prevents the authorized access to a wire or electronic communica-
tion while in electronic storage in such a system” shall be liable for damages. 18
U.S.C. § 2701(a); 18 U.S.C. § 2707 (providing for civil liability under the statute).
The statute further provides that “[i]t shall not be unlawful ... [to] access an elec-
tronic communication made through an electronic communication system that is
configured so that such electronic communication is readily accessible to the
general public.” 18 U.S.C. § 2511(2)(g)(i). In other words, the SCA covers: (1)
electronic communications, (2) that were transmitted via an electronic communica-
tion service, (3) that are in electronic storage, and (4) that are not public. Facebook
wall posts that are configured to be private meet all four criteria.

First, Facebook wall posts are electronic communications. The SCA defines
“electronic communication” as “any transfer of signs, signals, writing, images,
sounds, data, or intelligence of any nature transmitted in whole or in part by a
wire, radio, electromagnetic, photoelectronic or photooptical system.” 18 U.S.C.
§ 2510(12). To create Facebook wall posts, Facebook users transmit writing, im-
ages, or other data via the Internet from their computers or mobile devices to
Facebook’s servers. Thus, Facebook wall posts are electronic communications.

Second, Facebook wall posts are transmitted via an electronic communication
service. The SCA defines “electronic communication service” as “any service which
provides to users thereof the ability to send or receive wire or electronic communi-
cations.” 18 U.S.C. § 2510(15). Facebook provides its users with the ability to send
and receive electronic communications, including private messages and Facebook
wall posts.

Third, Facebook wall posts are in electronic storage. The SCA distinguishes
between two different types of electronic storage. The first is defined as “any tem-
porary, intermediate storage of a wire or electronic communication incidental to
the electronic transmission thereof.” 18 U.S.C. § 2510(17)(A). The second type of
storage is defined as “any storage of such communication by an electronic com-
munication service for purposes of backup protection of such communication.” 18
U.S.C. § 2510(17)(B). Unlike email, Facebook wall posts are not held somewhere
temporarily before they are delivered. Rather, the website itself is the final destina-
tion for the information. Thus, Facebook wall posts are not held in temporary, in-
termediate storage.

However, Facebook does store electronic communications for backup purposes.
When Facebook users post information, the information is immediately saved to a
Facebook server. When new posts are added, Facebook archives older posts on
separate pages that are accessible, but not displayed. Because Facebook saves and
archives wall posts indefinitely, the Court finds that wall posts are stored for back-up purposes. Accordingly, Facebook wall posts are in electronic storage.

Fourth, Facebook wall posts that are configured to be private are, by definition, not accessible to the general public. The touchstone of the Electronic Communications Privacy Act is that it protects private information. The language of the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private. See 18 U.S.C. § 2511(2)(g)(i) (there is no protection for information that is “configured [to be] readily accessible to the general public”). Cases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information. See Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding that SCA prevented Viacom from accessing YouTube “videos that [users] have designated as private and chosen to share only with specified recipients”); [Crispin v. Christian Audigier Inc., 717 F. Supp. 2d at 965, 991 (C.D. Cal. 2010)] (finding that SCA protection for Facebook wall posts depends on plaintiff’s use of privacy settings); cf. Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006) (“an express warning, on an otherwise publicly accessible webpage” is insufficient to give rise to SCA protection).

Facebook allows users to select privacy settings for their Facebook walls. Access can be limited to the user’s Facebook friends, to particular groups or individuals, or to just the user. The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are “configured to be private” for purposes of the SCA. The Court notes that when it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls. Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has. “Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing” and would be legally unworkable. Crispin, 717 F. Supp. 2d at 990.

At least one other court has determined that non-public Facebook wall posts are covered by the SCA, albeit in a slightly different context. In Crispin, the District Court for the Central District of California was asked to decide whether a third-party subpoena should be quashed under the SCA. The defendants in Crispin subpoenaed information located on the plaintiff’s MySpace and Facebook pages, including the plaintiff’s Facebook wall posts and MySpace comments. The plaintiff sought to quash the subpoena, arguing that the SCA prohibited Facebook and MySpace from disclosing the information. To determine whether the SCA applied to these communications, the court analogized a Facebook wall post to technology that existed in 1986: a posting on a BBS. A BBS could be configured to be public or private. If a BBS was configured to be private, access to the BBS was restricted to a particular community of users, and the messages posted to the BBS were only viewable by those users. The Crispin court recognized that there was a long line of cases finding that the SCA was intended to reach private BBS’s. Id. at 981 (collecting cases). The court then found that there was “no basis for distinguishing between a restricted-access BBS and a user’s Facebook wall or MySpace comments”: both technologies allowed users to post content to a restricted group of people, but not the public at large. Id. at 981. The court therefore concluded that, if the plaintiff’s Facebook page was configured to be private, then his wall posts were covered by the SCA. This Court agrees in all respects with the reasoning of Crispin.
Accordingly, the Court finds that non-public Facebook wall posts are covered by the SCA. Because Plaintiff in this case chose privacy settings that limited access to her Facebook wall to only her Facebook friends, the Court finds that Plaintiff’s Facebook wall posts are covered by the SCA.

ii. The SCA’s Authorized User Exception Applies in this Case

Having concluded that the SCA applies to the type of communication at issue in this case, the Court next evaluates whether either of the SCA’s statutory exceptions apply. The SCA “does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c); see also Pietrylo v. Hillstone Rest. Grp., No. 06–5754, 2009 WL 3128420, at *2 (D.N.J. Sept. 25, 2009) (“According to the SCA, if access to [a restricted website] was authorized by a user of that service with respect to a communication of or intended for that user, there is no statutory violation”). For the reasons set forth below, the Court finds that the authorized user exception (the second exception) applies in this case.

The authorized user exception applies where (1) access to the communication was “authorized,” (2) “by a user of that service,” (3) “with respect to a communication ... intended for that user.” 18 U.S.C. § 2701(c)(2). Access is not authorized if the ‘purported ‘authorization’ was coerced or provided under pressure.” Pietrylo, 2009 WL 3128420, at *3. In this case, all three elements of the authorized user exception are present.

First, access to Plaintiff’s Facebook wall post was “authorized.” 18 U.S.C. § 2701(c)(2). The undisputed evidence establishes that Ronco voluntarily provided Plaintiff’s Facebook posts to MONOC management without any coercion or pressure. Caruso testified at his deposition that Plaintiff’s Facebook friend Ronco voluntarily took screenshots of Plaintiff’s Facebook page and either emailed those screenshots to Caruso or printed them out for him. This information was completely unsolicited. Caruso never asked Ronco for any information about Plaintiff and never requested that Ronco keep him apprised of Plaintiff’s Facebook activity; in fact, Caruso was surprised that Ronco showed him Plaintiff’s Facebook postings. Caruso never had the password to Ronco’s Facebook account, Plaintiff’s Facebook account, or any other employee’s Facebook account. ...

Second, access to Plaintiff’s Facebook wall post was authorized “by a user of that service.” 18 U.S.C. § 2701(c)(2). A “user” is “any person or entity who (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use.” 18 U.S.C. § 2510(13). It is undisputed that Ronco was a Facebook user: Plaintiff acknowledged that she added Ronco as a Facebook friend and posted on Ronco’s Facebook wall.

Third, Plaintiff’s Facebook wall post was “intended for that user.” 18 U.S.C. § 2701(c)(2). Based on the privacy settings that Plaintiff selected for her Facebook page, Plaintiff’s wall posts were visible to, and intended to be viewed by, Plaintiff’s Facebook friends. On June 8, 2009, when Plaintiff posted the comment about the museum shooting, Ronco was one of Plaintiff’s Facebook friends. Thus, the post was intended for Ronco.

In conclusion, access to Plaintiff’s Facebook wall post was authorized by a Facebook user with respect to a communication intended for that user. Therefore, the authorized user exception applies and Defendants are not liable under the SCA. Accordingly, the motion for summary judgment on Count 1 is GRANTED. ...
QUESTIONS

1. *Ehling* provides a clear explanation of the SCA's ambit. But is the court's holding on the first crucial question – whether Wall posts are “in electronic storage” – convincing?

2. Does the SCA protect emails? Text messages? Skype calls taped and saved by one of the participants? Shared spreadsheets on Google Docs?

3. How much work are Facebook's privacy controls doing in this opinion? The court points to them to show both that Ehling’s posts were not “readily accessible to the general public” and that access to them was “authorized.” Are these holdings consistent?

4. Would the result change if Ehling testified that she misunderstood Facebook’s privacy controls and had not meant to share the post in question with Ronco? What if she made the post visible only to a few family members, but Facebook’s privacy settings subsequently changed so that it became visible to Ronco and her other co-workers?

PEN REGISTERS AND TRAP AND TRACE DEVICES

Title 18, United States Code

§ 3121 – General prohibition on pen register and trap and trace device use; exception

(a) In General. – Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978.

(b) Exception. – The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service –

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) Limitation. – A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) Penalty. – Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122 – Application for an order for a pen register or a trap and trace device
(a) Application. –

(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of Application. – An application under subsection (a) of this section shall include –

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3127 - Definitions for chapter

As used in this chapter – …

(3) the term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication; …

Questions

1. What is a pen register? A trap and trace device? How significant is the difference, if any, between the two? The statute refers to “dialing, routing, addressing, or signaling information”; what are these for a telephone? For a home Internet connection? For a VoIP service like Skype?
2. What legal standard must the government satisfy to obtain a pen register order? How does this compare to the standard for a wiretap order? Does this standard satisfy the Fourth Amendment?

**NOTE ON TECHNICAL ASSISTANCE**

Sometimes the government needs help to install a wiretap, a pen register, or other surveillance device. The best way to tap a phone line, for example, is at the phone company’s facilities, using its equipment. Thus, surveillance statutes generally contain provisions requiring that specified private parties provide “technical assistance” to the government. Consider, for example, the technical assistance provision of the Wiretap Act, 18 U.S.C. § 2518(4):

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.

In *The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003), the appellant operated a network for on-board navigation systems in luxury cars. The FBI obtained a § 2518 order compelling the appellant to activate the system in a particular car, turn on the microphone, and allow the FBI to listen in. The court held (over a dissent) that although § 2518 could apply to the appellant, this particular order required more than “a minimum of interference with the services” because it would disable the other functions of the navigation system.

There is a similar provision in the pen register statute, 18 U.S.C. § 3124, and you have already seen that the Stored Communications Act requires providers simply to turn over the target’s communications on receipt of a proper court order. The Communications Assistance to Law Enforcement Act (CALEA) goes even further: it requires that a “telecommunications carrier” (i.e. someone who provides “the transmission or switching of wire or electronic communications as a common carrier for hire”) be capable of complying with interception orders. 47 U.S.C. § 1002 So the phone company must design and operate its network so that it can provide the necessary technical assistance under Wiretap Act and pen register orders. CALEA provides, however, that it does not apply to “information services” (i.e., “generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications”), so as a result only providers of physical infrastructure tend to be subject to CALEA. It also provides that “A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”

Finally, there is the All Writs Act, initially enacted as part of the Judiciary Act of 1789, gives the federal courts the power to issue “all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651. In *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), the FBI wanted to install pen registers on two suspects’ telephone lines, but could only do so unobtrusively if the telephone company provided some
additional wiring. The Supreme Court held that the FBI could obtain an order under the All Writs Act directing the company to do so. The Court appeared to balance three factors: the closeness of the relationship of the company to the matter being investigated, the necessity of the order, and the burden on the company.

Most recently, the technical assistance debate has come to a head in fights over smartphone encryption. The FBI attempted to compel Apple to assist in unlocking an iPhone used by Syed Farook, who killed 14 people in San Bernardino on December 2, 2015. That case was mooted when the FBI paid more than $1.3 million to a third party for software that unlocked the phone. In another case, a magistrate judge rejected an All Writs Act demand for Apple’s assistance because between CALEA and the SCA (neither of which imposed such a duty on device manufacturers) there was no legislatively unforeseen gap for the court to fill with the All Writs Act. *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

**QUESTIONS**

1. In court and in the press, Apple has made broader arguments against compelled technical assistance: that the Apple is an uninvolved party and the burden on it is excessive, that requiring it to bypass the encryption on its devices creates a “backdoor” that makes everyone’s devices less secure, that requiring it to write software it disagrees with is a form of compelled speech prohibited by the First Amendment, and that compelling its engineers to write software for the government takes property without due process of law. How persuasive are these objections? If Apple has a constitutional right not to write encryption-cracking software, does Tesla have a constitutional right not to write software that makes left-turn signals?

2. How much can and should companies say when they receive surveillance orders? Many of the authorizing statutes allow the government to obtain nondisclosure orders prohibiting the company from disclosing the contents of the surveillance order? Are these orders unconstitutional restrictions on freedom of speech? Can a company subject to one publish an aggregate report listing the number and type of orders it has received for customer data in the past year? How about a so-called “warrant canary” stating, “We have not received any court orders for customer data. Watch closely for the removal of this notice.”?

**C. National Security**

Alongside the system of law enforcement surveillance discussed above there is a vast parallel system of national-security surveillance. Although the work is carried out by a variety of intelligence agencies and their international counterparts, it centered on, and has come to be identified with, the National Security Agency (NSA). This section sketches the legal framework governing national security surveillance, and some of the ways the NSA’s bulk surveillance programs complicate the story told above.

The discussion here will necessarily be incomplete, and not just because of space restrictions. The NSA is legendendarily secretive. Its unofficial nickname for many years was “No Such Agency,” and though it is now forthcoming about its own existence, both its activities and the legal authority it purports to act under are often highly classified. Some of the following came to light as a result of investiga-
tive journalism during the 2000s. Other information was revealed through the actions of whistleblowers, or under pressure from members of Congress concerned about the NSA’s actions, particularly Oregon senator Ron Wyden.

But the real catalyst for public discussion of the NSA’s surveillance programs was the extraordinary series of leaks by former NSA contractor Edward Snowden in the summer of 2013. While working as a technician on NSA information systems, he systematically downloaded thousands of documents. Snowden then reached out to investigative journalist Glenn Greenwald (then working with the British newspaper The Guardian) and began supplying Greenwald and other reporters with highly revealing slide decks, internal memoranda, legal opinions, and court orders describing the NSA’s programs. Other reporters working with or inspired by Snowden have also dug into the secretive world of NSA surveillance, and further information has been released by the government in response to their efforts – but much still remains unknown. This section draws heavily from the December 2013 report of a five-member committee appointed by President Obama to review the NSA’s surveillance programs, and from opinions issued by the Foreign Intelligence Surveillance Court in response to applications from the NSA and other law-enforcement and security agencies. But keep in mind that even these documents tell only part of the story.

The NSA is officially charged with “signals intelligence” – collecting information about the communications of the enemies of the United States, while safeguarding the United States’s own communications. Following World War II, military codebreaking operations were ultimately centralized in the NSA by President Truman in 1952. As electronic communications have grown in importance, so has the NSA’s role in intercepting them.

Modern oversight of the NSA dates to 1975, when the Senate formed a committee to study United States intelligence operations. The committee, known as the “Church Committee” after its chairman, Frank Church, produced a series of fourteen reports on widespread abuses by the intelligence agencies. In a project code-named MINARET, the NSA intercepted and monitored the contents of the communications of Americans, including Martin Luther King, Jr. and critics of the Vietnam war, without judicial oversight. And in a project codenamed SHAMROCK, the NSA collected all telegrams entering and leaving the United States, passing many of them along to other agencies. Congressional concern about these and other programs resulted in the passage of the Foreign Intelligence Surveillance Act of 1978, or FISA.

FISA attempted to safeguard the nation against the kinds of abuses that had been documented by the Church Committee, while at the same time preserving the nation’s ability to protect itself against external threats. FISA was a carefully designed compromise between those who wanted to preserve maximum flexibility for the intelligence agencies and those who wanted to place foreign intelligence surveillance under essentially the same restrictions as ordinary surveillance activities (at least insofar as the rights of Americans were concerned).
Chapter 4: Privacy

To that end, FISA brought foreign intelligence surveillance within a legal regime involving strict rules and structured oversight by all three branches of the government, but also granted the government greater freedom in the realm of foreign intelligence surveillance than it had in the context of others types of surveillance.

FISA restricted the government's authority to use electronic surveillance inside the United States to obtain foreign intelligence from "foreign powers." The term "foreign powers" was defined to include not only foreign nations, but also the agents of foreign nations and any "group engaged in international terrorism." FISA established the Foreign Intelligence Surveillance Court (FISC), consisting of seven (now eleven) federal judges appointed by the Chief Justice of the United States to serve staggered terms on the FISC. FISA provided that any government agency seeking to use electronic surveillance for foreign intelligence purposes inside the United States had to obtain a warrant from the FISC. For such a warrant to be issued, the government had to show "probable cause to believe that the target of the electronic surveillance" is an agent of a foreign power.

It is important to note several significant elements to this approach. First, by requiring the government to obtain a warrant from the FISC, FISA denied the President the previously assumed authority to engage in foreign intelligence surveillance inside the United States without judicial supervision. This was a major innovation.

Second, Congress created the FISC so it could deal with classified information and programs involved in foreign intelligence surveillance. Ordinary federal courts lacked the facilities and clearances to deal with such matters. A special court was therefore necessary if such classified matters were to be brought under the rule of law.

Third, FISA did not deal with the President's authority to engage in foreign intelligence activities outside the United States. FISA did not require the government to obtain a FISA warrant from the FISC before it could legally wiretap a telephone conversation between two Russians in Moscow or between a US citizen in France and a US citizen in England. In such circumstances, FISA left the issue, as in the past, to the Executive Branch, operating under the National Security Act of 1947, the National Security Agency Act of 1959, and the US Constitution.

Fourth, FISA did not limit the government's use of electronic surveillance in the foreign intelligence context to those situations in which the government has probable cause to believe that criminal activity is afoot. Rather, FISA permitted the government to engage in electronic surveillance in the United States to obtain foreign intelligence information as long as the government can establish to the satisfaction of the FISC that it has probable cause to believe that the "target" of the surveillance is an "agent of a foreign power."

These features of the system established by FISA reflect Congress' understanding at the time of the central differences between electronic surveillance for foreign intelligence purposes and electronic surveillance for traditional criminal investigation purposes. But in light of past abuses, the possibility of politicization, and the decision to authorize foreign intelligence surveillance of individuals, including American citizens, for whom there is no probable cause to suspect criminal conduct, FISA instituted a broad range of safeguards to prevent misuse of this authority.

For example, FISA requires the Attorney General to approve all applications for FISA warrants; it requires the Attorney General to report to the House and Senate
Intelligence Committees every six months on the FISA process and the results of FISA-authorized surveillance; it requires the Attorney General to make an annual report to Congress and the public about the total number of applications made for FISA warrants and the total number of applications granted, modified, or denied; and it expressly provides that no United States citizen or legal resident of the United States may be targeted for surveillance under FISA “solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” Finally, FISA requires the use of “minimization” procedures to protect the privacy rights of individuals who are not themselves “targets” of FISA surveillance but whose conversations or personal information are incidentally picked up in the course of electronic surveillance of legitimate targets under the Act.

FISA changed only modestly from 1978 until the events of September 11, 2001. Although FISA originally applied only to electronic surveillance, Congress gradually widened its scope to other methods of investigation. In 1995, it was extended to physical searches; in 1998, it was extended to pen register and trap-and-trace orders (which enable the government to obtain lists of the telephone numbers and e-mails contacted by an individual after the issuance of the order); and in that same year it was extended to permit access to limited forms of business records, including documents kept by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities, ...

FISA is not the only legal authority governing foreign intelligence activities. Other statutes and Executive Orders address other facets of the operations of the Intelligence Community. The National Security Act and other laws relating to specific agencies, such as the Central Intelligence Agency Act and the National Security Agency Act, regulate what agencies can do, and the Intelligence Community is also governed by laws such as the Privacy Act and the Electronic Communications Privacy Act.

Executive Order 12333 is the principal Executive Branch authority for foreign intelligence activities not governed by FISA. Executive Order 12333 specifies the missions and authorities of each element of the Intelligence Community; sets forth the principles designed to strike an appropriate balance between the acquisition of information and the protection of personal privacy; and governs the collection, retention, and dissemination of information about United States Persons (American citizens and non-citizens who are legal residents of the United States).

Executive Order 12333 authorizes the Attorney General to promulgate guidelines requiring each element of the Intelligence Community to have in place procedures prescribing how it can collect, retain, and disseminate information about US persons. The guidelines define each agency’s authorities and responsibilities. With respect to National Security Agency (NSA), for example, Executive Order 12333 designates NSA as the manager for Signals Intelligence (SIGINT) for the Intelligence Community, and the Attorney General’s Guidelines define how SIGINT may be conducted for collection activities not governed by FISA.

Section 2.4 of Executive Order 12333 prohibits specific elements of the Intelligence Community from engaging in certain types of activities inside the United States. The CIA, for example, is generally prohibited from engaging in electronic surveillance, and members of the Intelligence Community other than the FBI are generally prohibited from conducting non-consensual physical searches inside the United States. ...
Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons...

B. Foreign Intelligence Surveillance and Section 702

In general, the federal government is prohibited from intercepting the contents of private telephone calls and e-mails of any person, except in three circumstances. First, in the context of criminal investigations, Title III of the Electronic Communications Privacy Act authorizes the government to intercept such communications if a federal judge issues a warrant based on a finding that there is probable cause to believe that an individual is committing, has committed, or is about to commit a federal crime and that communications concerning that crime will be seized as a result of the proposed interception.

Second, as enacted in 1978, FISA authorized the federal government to intercept electronic communications if a judge of the FISC issues a warrant based on a finding that the purpose of the surveillance is to obtain foreign intelligence information, the interception takes place inside the United States, and there is probable cause to believe that the target of the surveillance is an agent of a foreign power (which includes, among other things, individuals engaged in international terrorism, the international proliferation of weapons of mass destruction, and clandestine intelligence activities).

Third, there is foreign intelligence surveillance that takes place outside the United States. At the time FISA was enacted, Congress expressly decided not to address the issue of electronic surveillance of persons located outside the United States, including American citizens, noting that the “standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States.” It was apparently assumed that intelligence collection activities outside the United States would be conducted under the Executive Branch’s inherent constitutional authority and the statutory authorizations granted to each Intelligence Community agency by Congress, and that it would be governed by presidential Executive Orders and by procedures approved by the Attorney General. To that end, in 1981 President Ronald Reagan issued Executive Order 12333, discussed above, which (as amended) specifies the circumstances in which the nation’s intelligence agencies can engage in foreign intelligence surveillance outside the United States.

Although Congress did not take up this issue in the immediate aftermath of the terrorist attacks of September 11, 2001, several developments brought the question to the fore. First, technological advances between 1978 and the early 21st century complicated the implementation of the original FISA rules. The distinction FISA drew between electronic surveillance conducted inside the United States and electronic surveillance conducted outside the United States worked reasonably well in 1978, because then-existing methods of communication and collection made that distinction meaningful. But the development of a global Internet communications grid with linchpins located within the United States undermined the distinction.

By the early twenty-first century, a large percentage of the world’s electronic communications passed through the United States, and foreign intelligence collection against persons located outside the United States was therefore increasingly conducted with the assistance of service providers inside the United States. Unless the legislation was amended, this new state of affairs meant that the government would have to go to the FISC to obtain orders authorizing electronic surveillance for foreign intelligence purposes even of individuals who were in fact outside the
United States, a state of affairs Congress had not anticipated at the time it enacted FISA in 1978.

Second, in late 2005 it came to light that, shortly after the attacks of September 11, President George W. Bush had secretly authorized NSA to conduct foreign intelligence surveillance of individuals who were inside the United States without complying with FISA. Specifically, the President authorized NSA to monitor electronic communications (e.g., telephone calls and e-mails) between people inside the United States and people outside the United States whenever NSA had “a reasonable basis to conclude that one party to the communication” was affiliated with or working in support of al-Qa’ida.

Because this secret program did not require the government either to obtain a warrant from the FISC or to demonstrate that it had probable cause that the target of the surveillance was an agent of a foreign power – even when the target was inside the United States – it clearly exceeded the bounds of what Congress had authorized in FISA. The Bush administration maintained that this program was nonetheless lawful, invoking both Congress’ 2001 Authorization to Use Military Force and the President’s inherent constitutional authority as commander-in-chief.

In light of these developments, Congress decided to revisit FISA. In 2007, Congress amended FISA in the Protect America Act (PAA), which provided, among other things, that FISA was inapplicable to any electronic surveillance that was “directed at a person reasonably believed to be located outside the United States.” In effect, the PAA excluded from the protections of FISA warrantless monitoring of international communications if the target of the surveillance was outside the United States, even if the target was an American citizen. The PAA was sharply criticized on the ground that it gave the government too much authority to target the international communications of American citizens.

The following year, Congress revised the law again in the FISA Amendments Act of 2008 (FAA). The FAA adopted different rules for international communications depending on whether the target of the surveillance was a “United States person” (a category that was defined to include both American citizens and non-citizens who are legal permanent residents of the United States) or a “non-United States person.” The FAA provides that if the government targets a United States person who is outside the United States, the surveillance must satisfy the traditional requirements of FISA. That is, the surveillance is permissible only if it is intended to acquire foreign intelligence information and the FISC issues a warrant based on a finding that there is probable cause to believe that the United States person is an agent of a foreign power, within the meaning of FISA. Thus, if the target of the surveillance is a United States person, the same FISA procedures apply – without regard to whether the target is inside or outside the United States.

On the other hand, the FAA provided in section 702 that if the target of foreign intelligence surveillance is a non-United States person who is “reasonably believed to be located outside the United States,” the government need not have probable cause to believe that the target is an agent of a foreign power and need not obtain an individual warrant from the FISC, even if the interception takes place inside the United States. Rather, section 702 authorized the FISC to approve annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that identify certain categories of foreign intelligence targets whose communications may be collected, subject to FISC-approved targeting and minimization procedures. The categories of targets specified by these certifications typ-
ically consist of, for example, international terrorists and individuals involved in the proliferation of weapons of mass destruction.

Under section 702, the determination of which individuals to target pursuant to these FISC-approved certifications is made by NSA without any additional FISC approval. In implementing this authority, NSA identifies specific “identifiers” (for example, e-mail addresses or telephone numbers) that it reasonably believes are being used by non-United States persons located outside of the United States to communicate foreign intelligence information within the scope of the approved categories (e.g., international terrorism, nuclear proliferation, and hostile cyber activities). NSA then acquires the content of telephone calls, e-mails, text messages, photographs, and other Internet traffic using those identifiers from service providers in the United States.

Illustrative identifiers might be an e-mail account used by a suspected terrorist abroad or other means used by by high-level terrorist leaders in two separate countries to pass messages. The number of identifiers for which NSA collects information under section 702 has gradually increased over time.

Section 702 requires that NSAs certifications attest that a “significant purpose” of any acquisition is to obtain foreign intelligence information (i.e. directed at international terrorism, nuclear proliferation, or hostile cyber activities), that it does not intentionally target a United States person, that it does not intentionally target any person known at the time of acquisition to be in the United States, that it does not target any person outside the United States for the purpose of targeting a person inside the United States, and that it meets the requirements of the Fourth Amendment. The annual certification provided to the FISC must attest that the Attorney General and the Director of National Intelligence have adopted guidelines to ensure compliance with these and other requirements under section 702, including that the government does not intentionally use section 702 authority to target United States persons, inside or outside the United States.135 The FISC annually reviews the targeting and minimization procedures to ensure that they satisfy all statutory and constitutional requirements.

Other significant restrictions govern the use of section 702:

- If a section 702 acquisition inadvertently obtains a communication of or concerning a United States person, section 702’s minimization procedures require that any information about such a United States person must be destroyed unless there are compelling reasons to retain it, for example, if the information reveals a communications security vulnerability or an imminent threat of serious harm to life or property.

- If a target reasonably believed to be a non-United States person located outside the United States either enters the United States or is discovered to be a United States person, acquisition must immediately be terminated.

- Any information collected after a non-United States person target enters the United States must promptly be destroyed, unless it constitutes evidence of criminal conduct or has significant foreign intelligence value.

- Any information collected prior to the discovery that a target believed to be a non-United States person is in fact a United States person must be promptly destroyed, unless it constitutes evidence of criminal conduct or has significant foreign intelligence value.

- The dissemination of any information about a United States person collected during the course of a section 702 acquisition is prohibited, unless it is
necessary to understand foreign intelligence or assess its importance, is evidence of criminal conduct, or indicates an imminent threat of death or serious bodily injury.

Section 702 imposes substantial reporting requirements on the government in order to enable both judicial and congressional oversight, in addition to the oversight conducted within the Executive Branch...

Although compliance issues under section 702 have been infrequent, they have been vexing when they arise. In one instance, the FISC held that, for technical reasons concerning the manner in which the collection occurred, the minimization procedures that applied to NSA’s upstream collection of electronic communications did not satisfy the requirements of either FISA or the Fourth Amendment. This was so because NSA’s use of upstream collection often involves the inadvertent acquisition of multi-communication transactions (MCTs), many of which do not fall within the parameters of section 702. Judge John Bates of the FISC noted that the “government’s revelations regarding the scope of NSA’s upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to ‘engage[ ] in electronic surveillance under color of law except as authorized’ by statute. . . .”

Judge Bates observed that “NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702” and that the vast majority of those communications are “not at issue here.” But, he added, the upstream collection represents “approximately 9 percent of the total Internet communications being acquired by NSA under Section 702,” and those acquisitions inadvertently sweep in “tens of thousands of wholly domestic communications” because they happen to be contained within an MCT that includes a targeted selector.

In such circumstances, Judge Bates noted that the “fact that NSA’s technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications . . . does not render NSA’s acquisition of those transactions ‘unintentional.’” Judge Bates concluded that “NSA’s minimization procedures, as applied to MCTs,” did not meet the requirements of either FISA or the Fourth Amendment. He therefore refused to approve NSA’s continuing acquisition of MCTs. Thereafter, the government substantially revised its procedures for handling MCTs, and in November 2011 Judge Bates approved the future acquisition of such communications subject to the new minimization standards. In addition, NSA took the additional step of deleting all previously acquired upstream communications.

According to NSA, section 702 “is the most significant tool in NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world.” To cite just one example, collection under section 702 “was critical to the discovery and disruption” of a planned bomb attack in 2009 against the New York City subway system” and led to the arrest and conviction of Najibullah Zazi and several of his co-conspirators. ...

OTHER SURVEILLANCE PROGRAMS

Tracing the government’s surveillance programs – and their legal status – is a challenging task. Any given surveillance program could be collected using multiple different techniques (e.g. secret overseas wiretaps or court orders to telecommunications companies), could be justified under multiple different legal authorities (e.g., Executive Order 12333 or FISA’s pen-register provisions), and could be carried out by multiple different agencies (e.g., the NSA, the CIA, or the FBI). The details
have come to light only in fragments, and existing programs have frequently been modified or placed on different legal foundations. In addition, even when some facts about a program have leaked, the government often refuses to confirm their authenticity and does its best to keep further details out of court. Here are a few of the many programs that have come to light:

- The **PRISM** program targets Internet communications as they pass through the United States. The NSA collects emails, videos, photos, chats, stored files, and other data from major Internet companies including Microsoft, Google, Yahoo!, Facebook, and Apple. Following the passage of the FISA Amendments Act, **PRISM** collection now takes place under Section 702 pursuant to directives approved by the FISC. As summarized by the Privacy and Civil Liberties Oversight Board:

  [A]n example using a fake United States company (“USA-ISP Company”) may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address “johntarget@usa-ISP.com” to communicate with associates about his efforts to engage in international terrorism. The NSA ... “tasks” johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target’s involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government “detasks” johntarget@usa-ISP.com.

  **Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act** 34 (2014).

- A variety of “upstream collection” programs collect data as it passes through telecommunications networks. Upstream collection of telephone calls are essentially wiretaps carried out in the middle of the phone network rather than at the target’s phone; upstream collection of Internet traffic involves installing specialized interception devices in the facilities of Internet backbone providers. Both are carried out under Section 702 directives approved by the FISC. The information collected on Internet communications is in some ways broader:

  Upstream collection acquires Internet transactions that are “to,” “from,” or “about” a tasked selector. With respect to “to” and “from” communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an “about” communication. An “about” communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication. If the NSA therefore applied its targeting procedures to task email address “JohnTarget@example.com,” to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email
address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name “John Target.”

*Id.* at 37. Although upstream collection is primarily based on the compelled assistance of United States telecommunications companies, the government has in place several ways of carrying it out abroad, including through partnerships between domestic and foreign telecommunications providers and under other legal authorities.

- The *muscular* program intercepted communications inside Google and Yahoo! networks. It was conducted in collaboration with the United Kingdom intelligence agency GCHQ and involved interceptions outside of the United States. It took advantage of the fact that while data was encrypted while being sent to and from users, it was unencrypted while being sent from one data center to another. In response, Google and Yahoo! began encrypting their internal traffic. It is not known whether the NSA has found a way to continue this surveillance.

- The NSA’s Tailored Access Operations unit specializes in installing surveillance software directly on targets’ networks and computers using exploits and other vulnerabilities. One of its programs, *quantum*, allows the NSA to impersonate websites, delivering malware to selected users who attempt to visit those sites.

- The *mystic* program records every telephone call to and from an unspecified foreign nation and stores them for thirty days.

- Various programs attempt to extract information from smartphone apps such as Angry Birds and Google Maps. *Noisy Smurf* is the codename for a tool that turns on a phone’s microphone to listen in to communications.

- All of these collection efforts feed into massive databases. Searching and analyzing these databases to extract patterns of interest is itself a major challenge. The NSA has abandoned some projects – such as an earlier program to collect Internet metadata – because of an inability to extract information with intelligence value from the masses of collected data. Programs like *XKeyscore* attempt to give intelligence analysts the tools to sift through the volumes of collected data and then to drill down and examine the communications of targets of interest in detail.

### LEGAL CHALLENGES TO NSA SURVEILLANCE

The litigation over the surveillance programs is equally complex. In 2005, after the *New York Times* revealed the existence of telephone and Internet surveillance programs under the name of the “Terrorist Surveillance Program” (TSP), a former AT&T technician, Mark Klein, went public with the existence of Room 641A at AT&T’s Folsom Street building in San Francisco, where NSA upstream collection took place. Based on Klein’s claims, the Electronic Frontier Foundation filed a class-action, alleging that AT&T violated the Constitution, the Wiretap Act, the Stored Communications Act, and other laws. The government resisted the suit, asserting the state secrets doctrine, which applies when “the evidence will expose military matters which, in the interest of national security, should not be divulged.” *United States v. Reynolds*, 345 U.S. 1, 10 (1953). The District Court allowed the
suit to proceed, *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 97 (N.D. Cak. 2006), and the decision was on appeal to the Ninth Circuit when the FISA Amendments Act passed in 2008.

With more than 40 cases pending against telecommunications companies for their role in TSP, the debate in Congress over what to do with it took on a special urgency. The FISA Amendments Act as passed included a blanket retroactive immunity, effectively terminating the litigation against the companies. The *Hepting* Plaintiffs challenged Congress's authority to confer retroactive immunity, but without success. *In re National Security Agency Telecommunications Records Litigation*, 671 F.3d 881 (9th Cir. 2011).

Now, challenges were brought against the government itself. Most notably, the same day that the FISA Amendments Act created Section 702, a coalition of human-rights and media groups sued to block it, claiming it violated the First and Fourth Amendments. But the Supreme Court held they lacked standing to sue. *Clapper v. Amnesty Int'l USA*, 113 S. Ct. 1138 (2013). Section 702 and other legal authorities merely provided a framework for surveillance. Their existence did not show that any surveillance was taking place. What was publicly known about the government's actual surveillance programs was too vague and fragmentary to establish that those programs reached any particular people or communications. Thus, the plaintiffs had “no actual knowledge of the Government's ... targeting practices” but could “merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired.” *Id.* at 1148.

*Clapper* was decided in February of 2013, and seemed to sound a death knell for anti-NSA litigation. But only a few months later, Edward Snowden upended all of that. The first stories based on the internal NSA documents he leaked were published on June 6, 2013, simultaneously by the *Guardian* and the *Washington Post*. And the first story was a blockbuster: the FISC had issued an order to Verizon Business Network Services to produce all of its call records for the period from April 25, 2013 to July 19, 2013. That was a game-changer, because it established the factual predicate of likely surveillance that had been missing in *Clapper*. Lawsuits followed, and some plaintiffs now had standing. See *Wikimedia Foundation v. NS4*, 857 F.3d 193 (4th Cir. 2017); *Schuchardt v. President of the United States*, 839 F.3d 336 (3d Cir. 2016). But in *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), the Ninth Circuit held that section 702 surveillance was constitutional, and so was the use of evidence thereby obtained in the criminal prosecution of the defendant. There, the government's section 702 surveillance targeted a non-U.S. person located outside the United States, and Mohamud's emails with that person were collected incident to that surveillance. The court was unconcerned with the greater scope of section 702 surveillance as compared with more traditional methods. Litigation over NSA surveillance programs continues.

**QUESTIONS**

1. Which of the following should the NSA attempt to wiretap:
   - Ayman al-Zawahiri, the leader of al Qaeda?
   - Vladimir Putin, the president of Russia?
   - Angela Merkel, the chancellor of Germany?
   - Rand Paul, senator from Kentucky and potential presidential candidate?
   - Drug gang leaders in the United States?
2. Intelligence acquisition is a complicated business. Some wiretaps require the cooperation of companies in the United States and abroad. Others are carried out surreptitiously (and sometimes illegally according to other countries’ laws) by breaking into facilities or through wireless surveillance. (For example, the NSA has tapped the internal networks of major Internet companies like Google.) Still others require creating software to break into the computers of intelligence targets. What kind of rules should govern how the NSA intercepts communications?

3. In addition to its offensive mission of conducting surveillance on foreign targets, the NSA has a defensive mission of protecting American targets from foreign surveillance. It advises other agencies on network security, and it provides input into private-sector cryptographic standard-setting. Some have alleged that this dual mission creates a conflict of interest and that the two missions should be separated into different agencies. Do you agree?

4. If the NSA has detailed records stored anyway, should the FBI, DEA, and other law-enforcement agencies be able to use them in criminal investigations? Should criminal defendants be able to obtain them in discovery – for example, to establish an alibi at the time of the crime?

**ZIPPER PROBLEM**

Senator Bernard Abbott (R-TX) has become concerned about the balance of power in the cryptography world. He is afraid that criminals, terrorists, and foreign powers can too easily spy on Americans’ communications – and that they’re also using encryption to keep their own nefarious plans hidden. Accordingly, he is preparing legislation to standardize American cryptography. His bill would:

1. Require all telephones (land-line and cellular) and Internet connections in the U.S. to be built with a new, standard encryption technology called Zipper. Devices using Zipper would have unique ID numbers; whenever two Zipper devices establish a connection, they will use their unique IDs to negotiate a secret key to encrypt their communications. The two Zipper devices will be able to turn the encrypted message back into intelligible sounds, images, text or whatever, but anyone eavesdropping on the connection will see only random 1s and 0s.*

2. Well, *almost* anyone. The U.S. government will manage a “key escrow database” that contains a second secret key for each unique Zipper ID number. Zipper will be designed in such a way that the government, using the second secret key, can also decrypt the communications. This database will be kept secure; a court order will be needed to allow law enforcement to look up the secret key for any given Zipper device.

3. In order to keep the system from breaking down, it will also be necessary to restrict the use of non-Zipper cryptography. Accordingly, after the imple-

* Yes, this actually works! The basic idea is a technique by the name of “Diffie-Hellman key exchange”; the math behind it is simple but a little mind-blowing. Its inventors, as the name suggests, are the same guys who invented public-key cryptography. An accessible video explanation of the technique is available at https://www.youtube.com/watch?v=3QnD2c4Xovk.
You are on the legal staff of SETEC, a non-profit advocacy group whose mission is to “keep the Internet open, free, and safe.” You have just learned about Senator Abbott’s proposal. You are flying to Washington for a meeting with the Senator’s staff tomorrow. Is the bill a good idea? Should you support it, oppose it, or push for modifications? What arguments will you make to the Senator’s staff, and how do you expect them to respond?

D. Anonymity

Our next topic has to do not with the contents of online communications, but rather with the identity of individuals using the Internet. The materials in this section consider what legal tests apply when one Internet user seeks to learn the real-life identity of another.

A short review of some of the technical aspects of Internet identity may be helpful. To communicate on the Internet, you need at the very least an IP address – and that address can then be used as a crucial link in identifying you. IP addresses are assigned to ISPs in blocks; ISPs generally keep records of which IP addresses they assigned to which subscribers and when.

To be sure, it is often possible to forge your IP address when sending messages. But then anyone trying to respond to your message will send their response to the wrong address. Thus, forged IP addresses are nearly useless for any interactive protocol – including, for example, HTTP for web browsing. The biggest use of forged IP addresses is in committing denial of service attacks: if your only goal is to overload a target computer, you don’t particularly care what it has to say in response.

There are other, more robust ways to communicate while obscuring your IP address from the computer you are trying to reach. They all require giving your IP address to an intermediary – here called a proxy – that forwards your packets on to the destination, listing its own IP address as the place to send responses. The proxy stands between the two endpoints; each talks only to the proxy, rather than directly to the other. Particularly if your traffic is encrypted on its way to the proxy (as it is on a “virtual private network” or “VPN”), this is good enough for many purposes. The BBC, for example, makes its shows available online, but only to viewers inside the United Kingdom, so American fans of the BBC have been known to use proxies that make it appear they are inside the U.K.

Proxies, however, require that the user trust the proxy at least with her IP address. For some, this is too much trust. More sophisticated systems will bounce messages through multiple proxies, so that anyone trying to track down a user must work through all of the proxies. At the highest level of security, onion routing systems like Tor separately encrypt each layer of the communication: each proxy except the last knows only that it is somewhere in the middle of a chain, and has no idea of the contents of the message. But even these systems don’t guarantee anonymity. In December 2013, Harvard University received a bomb threat during final exams; the threat was emailed by a Tor user. Rather than trying to trace him back one hop at a time (through many potentially uncooperative nodes), Harvard checked its own network records and found that exactly one student had been us-
ing Tor at the relevant time. When questioned by an FBI agent, the student confessed.

IP addresses are hardly the only digital identifiers at work online. Email addresses are an obvious example; so are usernames. Cookies (discussed below in the next section) identify a web user’s browser uniquely over time; it is also possible to use other details, such as the list of fonts a user has installed, to uniquely fingerprint a particular web user’s browser. Cell phones and other mobile devices have unique hardware identifiers, as do the SIM cards they use to connect to a cellular network. And any device communicating on an Ethernet or Wi-Fi network has a unique “media access control” address, commonly known as a MAC address. But because these are local rather than global networks, it is technically easy to change one’s MAC address with few untoward consequences.

**STORED COMMUNICATIONS ACT**

[Refer back to the SCA excerpts, *supra*.]

**QUESTIONS**

1. The basic rule on voluntarily disclosing the identity of a user is set forth in 18 U.S.C. § 2702(a)(3). Suppose that you work for Hotmail. You have just received a letter from the NYPD requesting the real name, address, and any other relevant contact information of the user with the email address “ThinBlueLiar@hotmail.com.” How should you respond? Why? What if the letter came from the Whole Foods Market corporation instead?

2. A second rule in § 2703 deals with required disclosures. If you work for the NYPD and you want to compel Hotmail to disclose the subscriber information for ThinBlueLiar, can you, and if so, how? What if you work for Whole Foods Market?

**JUKT MICRONICS PROBLEM**

You are an Assistant U.S. Attorney assigned to help the FBI investigate a computer intrusion at Jukt Micronics, which designs and manufactures circuit boards for high-performance scientific computing in physics and chemistry labs. Recently, someone has managed to gain access to – and overwrite – a file containing the prototype design for the JK-478, the company’s next big project. The file was replaced with a pornographic picture which was captioned, “THE BIG BAD BIONIC BOY HAS BEEN HERE BABY.”

This morning, the firm’s CEO received an email from eatmyjukt@hiert.com. Hiert.com is an ad-supported web email system: users don’t need to supply anything more than a desired username and password to create an account. The email’s author, “Ian,” claimed to be responsible for the computer intrusion and to have the original file in his possession. He demanded $250 million for its return. The number is obviously outrageous – Jukt’s entire annual revenues are only about $40 million. You and your FBI contact are starting to suspect you’re dealing with a talented (and possibly underage) amateur.

Leaving aside other possible investigative avenues, how should you attempt to turn “eatmyjukt” into an actual name and address so that the FBI can ask “Ian” some questions? How likely is this process to succeed? What could go wrong? Your strategy should consider both the technical and legal aspects of the problem. *(Hint: The technical part will take more than one step. The legal part is straight-
DOE I v. INDIVIDUALS, Whose True Names Are Unknown*

Droney, District Judge:

On February 1, 2008, the plaintiffs, Jane Doe I and Jane Doe II (the “Does”) issued a subpoena *duces tecum*† to SBC Internet Services, Inc., now known as AT&T Internet Services (“AT&T”), the internet service provider, for information relating to the identity of the person assigned to the Internet Protocol (“IP”) address from which an individual using the pseudonym “AK47” posted comments on a website. The individual whose internet account is associated with the IP address at issue, referring to himself as John Doe 21, has moved to quash that subpoena. John Doe 21 has also moved for permission to proceed anonymously in this matter.

I. Background

This action was brought by Doe I and Doe II, both female students at Yale Law School, against unknown individuals using thirty-nine different pseudonymous names to post on a law school admissions website named AutoAdmit.com (“AutoAdmit”). The plaintiffs allege that they were the targets of defamatory, threatening, and harassing statements posted on AutoAdmit from 2005 to 2007.

AutoAdmit is an internet discussion board on which participants post and review comments and information about undergraduate colleges, graduate schools, and law schools. It draws between 800,000 and one million visitors per month. Anyone who can access the internet can access AutoAdmit and view the messages posted on its discussion boards. Individuals who register with AutoAdmit, which can be done under real or assumed names, may post new messages and respond to the messages of other registered users. When a participant posts a new message, any further comments or responses to that message are collected as a “thread.” Messages and threads containing certain words or subject matter can be found by searching for those words using an internet search engine.

The first message about Doe II that appeared on AutoAdmit was posted on January 31, 2007, by an anonymous poster. The message linked to a photograph of Doe II and encouraged others to “Rate this HUGE breasted cheerful big tit girl from YLS.” After this message was posted, dozens of additional messages about Doe II appeared in the thread. These messages contained comments on Doe II’s breasts and the posters’ desire to engage in sexual relations with her. Certain of the posters appeared to be Doe II’s classmates at Yale Law School because of personal information they revealed. The posts regarding Doe II continued throughout the

---

* [Ed: This case involves allegations of online harassment and threats of violence.]
† [Ed: A subpoena is a court order demanding that the recipient appear or produce specified documents. Subpoenas aren’t subject to judicial oversight before they issue. *See* Fed. R. Civ. Proc. 45(a)(3) (“The clerk must issue a subpoena, signed but otherwise in blank, to a party who requests it. That party must complete it before service.”) Instead, the proper response from the recipient of an improper subpoena is a motion to *quash* (not “squash”) it.]
1 Because John Doe 21 chose a male pseudonymous name to proceed under, the Court will refer to John Doe 21 using male pronouns. This does not reflect a finding by the Court that John Doe 21 is indeed male.
winter and spring of 2007, and included statements, for example, that she fantasized about being raped by her father, that she enjoyed having sex while family members watched, that she encouraged others to punch her in the stomach while seven months pregnant, that she had a sexually transmitted disease, that she had abused heroin, and that a poster “hope[s] she gets raped and dies.” On March 9, 2007, a poster sent an email directly to Doe II and at least one member of the Yale Law School faculty describing the alleged criminal history of Doe II’s father. This message was also posted on AutoAdmit.

By March, nearly two hundred threads had been posted about Doe II on AutoAdmit. It is in this context that an anonymous poster under the moniker “AK47,” known on AutoAdmit for posting threatening and derogatory comments about minority groups, posted a message falsely stating “Alex Atkind, Stephen Reynolds, [Doe II], and me: GAY LOVERS.”

The posting of comments regarding Doe II continued into April and May of 2007, including one message which the poster claimed had also been sent to Doe II’s future employer which recounted some of the claims made about Doe II on AutoAdmit. On June 8, 2007, Doe II, along with Doe I, filed the complaint in the instant action, alleging libel, invasion of privacy, negligent and intentional infliction of emotional distress, and copyright violations. Doe II’s complaint described the harm and results she experienced because of the comments about her on AutoAdmit, including treatment for severe emotional distress, interference with her educational progress, reputational harm, and pecuniary harm.

The news of the filing of the Does’ complaint quickly became a subject of discussion on AutoAdmit. AK47, for example, wrote a post concerning his opinion on the merits of the plaintiffs’ case, and wondered whether posters were “allowed to use [Doe II’s] name in thread’s anymore.” Subsequently, on June 17, 2007, AK47 posted the statement “Women named Jill and Doe II should be raped.” On June 24, 2007, AK47 started a thread entitled “Inflicting emotional distress on cheerful girls named [Doe II].”

On February 1, 2008, the plaintiffs issued a subpoena duces tecum to AT&T for information relating to the identity of the person assigned to the IP address from which an individual using the pseudonym “AK47” posted comments on AutoAdmit about Doe II. This subpoena was issued in accordance with this Court’s order of January 29, 2008, which granted the Does’ motion to engage in limited, expedited discovery to uncover the identities of the defendants in this case. On February 7, 2008, AT&T sent a letter to the person whose internet account corresponded with the IP address at issue, John Doe 21 (“Doe 21”), notifying Doe 21 that it had received a subpoena ordering it to produce certain information relating to Doe 21’s internet account. The letter stated that Doe 21 could file a motion to quash or for a protective order before the date of production, which was February 25, 2008, and that AT&T must receive a copy of such a motion prior to that date. Doe 21 filed the instant motion to quash on February 25, 2008, and on February 26, 2008, AT&T complied with the subpoena. On March 12, 2008, Doe 21 filed his motion to proceed anonymously.

Because Doe 21 does not have counsel and his true identity is yet unknown to the Court, the Court appointed pro bono counsel to represent the interests of Doe 21 at oral argument on the instant motions, which took place on May 5, 2008.
Chapter 4: Privacy

II. Motion to Quash

A. Threshold Issues ...

2. Mootness

Doe II argues that the motion to quash is moot because the information sought has already been turned over to the plaintiffs by AT&T. However, the Court rejects this argument because the plaintiffs can be ordered to return the information and be prohibited from using it. See Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556, 561 (S.D.N.Y. 2004).

B. Merits of the Motion to Quash

A subpoena shall be quashed if it “requires disclosure of privileged or other protected matter and no exception or waiver applies.” Fed.R.Civ.P. 45(c)(3)(A)(iii). Doe 21 moves to quash the subpoena because he claims disclosure of his identity would be a violation of his First Amendment right to engage in anonymous speech.

The First Amendment generally protects anonymous speech. ... The United States Supreme Court has also made clear that the First Amendment’s protection extends to speech on the internet. ... Courts also recognize that anonymity is a particularly important component of Internet speech. “Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas[;] ... the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.” Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1092, 1097 (W.D. Wash. 2001). However, the right to speak anonymously, on the internet or otherwise, is not absolute and does not protect speech that otherwise would be unprotected. See, e.g., ... In re Subpoena Duces Tecum to America Online, Inc., No. 40570, 2000 WL 1210372, at *6 (Va. Cir. Ct. 2000) (“Those who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights.”). ...

The forgoing principles and decisions make clear that Doe 21 has a First Amendment right to anonymous Internet speech, but that the right is not absolute and must be weighed against Doe II’s need for discovery to redress alleged wrongs. Courts have considered a number of factors in balancing these two competing interests. This balancing analysis ensures that the First Amendment rights of anonymous Internet speakers are not lost unnecessarily, and that plaintiffs do not use discovery to “harass, intimidate or silence critics in the public forum opportunities presented by the Internet.” Dendrite Intern. Inc. v. Doe No. 3, 775 A.2d 756, 771 (2001). The Court will address each factor in turn.

First, the Court should consider whether the plaintiff has undertaken efforts to notify the anonymous posters that they are the subject of a subpoena and withheld action to afford the fictitiously named defendants a reasonable opportunity to file and serve opposition to the application. ... In this case, the plaintiffs have satisfied this factor by posting notice regarding the subpoenas on AutoAdmit in January of 2008, which allowed the posters ample time to respond, as evidenced by Doe 21’s activity in this action.

Second, the Court should consider whether the plaintiff has identified and set forth the exact statements purportedly made by each anonymous poster that the plaintiff alleges constitutes actionable speech. ... Doe II has identified the allegedly actionable statements by AK47/Doe 21: the first such statement is “Alex Atkind, Stephen Reynolds, 255 [Doe II], and me: GAY LOVERS;” and the second such
statement is “Women named Jill and Doe II should be raped.” The potential liability for at least the first statement is more fully discussed below.

The Court should also consider the specificity of the discovery request and whether there is an alternative means of obtaining the information called for in the subpoena. ... Here, the subpoena sought, and AT&T provided, only the name, address, telephone number, and email address of the person believed to have posted defamatory or otherwise tortious content about Doe II on AutoAdmit, and is thus sufficiently specific. Furthermore, there are no other adequate means of obtaining the information because AT&T's subscriber data is the plaintiffs' only source regarding the identity of AK47.

Similarly, the Court should consider whether there is a central need for the subpoenaed information to advance the plaintiffs' claims. ... Here, clearly the defendant's identity is central to Doe II's pursuit of her claims against him.

Next, the Court should consider the subpoenaed party's expectation of privacy at the time the online material was posted. ... Doe 21's expectation of privacy here was minimal because AT&T's Internet Services Privacy Policy states, in pertinent part: “We may, where permitted or required by law, provide personal identifying information to third parties . . . without your consent . . . To comply with court orders, subpoenas, or other legal or regulatory requirements.” Thus, Doe 21 has little expectation of privacy in using AT&T's service to engage in tortious conduct that would subject him to discovery under the federal rules.

Finally, and most importantly, the Court must consider whether the plaintiffs have made an adequate showing as to their claims against the anonymous defendant. Courts have differed on what constitutes such an adequate showing. Several courts have employed standards fairly deferential to the plaintiff, requiring that the plaintiff show a “good faith basis” to contend it may be the victim of conduct actionable in the jurisdiction where the suit was filed; ... ; or to show that there is probable cause for a claim against the anonymous defendant. ... The Court finds these standards set the threshold for disclosure too low to adequately protect the First Amendment rights of anonymous defendants, and thus declines to follow these approaches.

Other courts have required that a plaintiff show its claims can withstand a motion to dismiss. ... However, other courts have rejected this procedural label as potentially confusing because of the variations in the motion to dismiss standard in different jurisdictions. ... Similarly, but more burdensome, some courts have used a standard which required plaintiffs to show their claims could withstand a motion for summary judgment. ... The Court finds this standard to be both potentially confusing and also difficult for a plaintiff to satisfy when she has been unable to conduct any discovery at this juncture. Indeed, it would be impossible to meet this standard for any cause of action which required evidence within the control of the defendant.

Several courts have required that a plaintiff make a concrete showing as to each element of a prima facie case against the defendant. ... Under such a standard, “[w]hen there is a factual and legal basis for believing [actionable speech] has occurred, the writer's message will not be protected by the First Amendment.” ... The Court finds such a standard strikes the most appropriate balance between the First Amendment rights of the defendant and the interest in the plaintiffs of pursuing their claims, ensuring that the plaintiff “is not merely seeking to harass or embarrass the speaker or stifle legitimate criticism.” ...
Doe II has presented evidence constituting a concrete showing as to each element of a prima facie case of libel against Doe 21. Libel is written defamation. To establish a prima facie case of defamation under Connecticut law, the Doe II must demonstrate that: (1) Doe 21 published a defamatory statement; (2) the defamatory statement identified the plaintiff to a third person; (3) the defamatory statement was published to a third person; and (4) the plaintiff's reputation suffered injury as a result of the statement. ...

A defamatory statement is defined as a communication that tends to “harm the reputation of another as to lower him in the reputation of the community or to deter third persons from associating or dealing with him . . .” Doe II alleges, and has presented evidence tending to show that, AK47's statement, “Alex Atkind, Stephen Reynolds, [Doe II], and me: GAY LOVERS,” is defamatory, because any discussion of Doe II's sexual behavior on the internet tends to lower her reputation in the community, particular in the case of any potential employers who might search for her name online. In fact, in the similar context of slander (spoken defamation), any statement that imputes “serious sexual misconduct” to a person subjects the publisher to liability, without any need to prove the special harms required for other slanderous speech. See 3 Restatement (Second), Torts § 574, at 195–96.

Doe II has also alleged and presented evidence that Doe 21's statement clearly identified Doe II by name and was available to a large number of third persons (peers, colleagues, potential employers), whether they were on Autoadmit for their own purposes, or searched for Doe II via a search engine. Finally, Doe II has alleged and provided evidence that her reputation did suffer injury because of this comment. In her interviews with potential employers in the Fall of 2007, Doe II felt she needed to disclose that existence of this and other such comments on AutoAdmit and explain that she had been targeted by pseudonymous online posters. In addition, this statement has contributed to difficulties in Doe II's relationships with her family, friends, and classmates at Yale Law School.

Thus, the plaintiff has shown sufficient evidence supporting a prima facie case for libel, and thus the balancing test of the plaintiff's interest in pursuing discovery in this case outweighs the defendant's First Amendment right to speak anonymously. The defendant's motion to quash is denied.

**QUESTIONS**

1. Note the case caption: *Doe v. Individuals*. The plaintiffs are attempting to proceed anonymously, while asking the court to reveal publicly the identities of the defendants. Is this fair? Why does each side seek to remain anonymous?

2. Doe 21 has filed a motion to quash but the subpoena was actually issued to AT&T. Why didn't AT&T move to quash? Could it have? How did Doe 21 find out about the subpoena?

---

7 Context is relevant in determining the meaning of a statement. See 3 Restatement (Second), Torts 563, at 163. Doe 21 suggests that the context in which the statements were made also shows that they were not defamatory, because AutoAdmit is well-known as a place for inane discussion and meaningless derogatory postings, such that one would not take such a statement seriously. However, not everyone who searched for Doe II's name on the internet, or who came across the postings on AutoAdmit, would be aware of the site's alleged reputation. Thus, Doe II has put forth sufficient evidence for a prima facie case of defamation.
3. The critical question of law in Doe v. Individuals is the standard the court should use in deciding whether the plaintiffs have made an “adequate showing as to their claims against the anonymous defendant.” Civil procedure gives us plenty of familiar standards. For example, the court could use a motion to dismiss standard, asking whether the plaintiff has pleaded all the elements of a valid cause of action. Or the court could use a summary judgment standard: the plaintiff must introduce sufficient uncontroverted evidence to prove every element of her claim. What are the advantages and disadvantages of these different tests? What standard does the court settle on?

4. Courts are usually good at fact-finding, but courts in unmasking cases are often visibly uncomfortable. Why? What's missing in a John Doe case that makes the judicial task significantly more difficult?

5. You have been retained by Liskula Cohen, a fashion model who lives in New York. Someone created a blog named “Skanks of NYC” on Google’s Blogspot blog hosting service. It consists entirely of posts about Cohen, such as:

   I would have to say that the first place award for “Skankiest in NYC” would have to go to Liskula Gentile Cohen. How old is this skank? 40 something? She’s a psychotic, lying, whoring, still going to clubs at her age, skank ...
   Yeah she may have been hot 10 years ago, but is it really attractive to watch this old hag straddle dudes in a nightclub or lounge? Desperation seeps from her soul, if she even has one.

Your client strongly suspects that the author of the blog is someone she knows. She is not interested in litigating a full case, but she would like to find out who is responsible for this “disgusting, scurrilous trash,” as she calls it. A friend of hers suggested filing a John Doe suit for defamation against the anonymous author, serving a subpoena for the author's identity on Google, and then dropping the lawsuit once the poster's identity has been revealed. Is this a good idea?

E. Consumer Privacy

Our next topic is the personal privacy issues that arise out of ordinary web use. What do websites know about you, what can they do with that information, and what information do you expose about yourself to the world?

IN RE DOUBLECLICK INC. PRIVACY LITIG.
154 F. Supp. 2d 497 (S.D.N.Y. 2001)

Buchwald, District Judge:

Plaintiffs bring this class action on behalf of themselves and all others similarly situated against defendant DoubleClick, Inc. (“defendant” or “DoubleClick”) seeking injunctive and monetary relief for injuries they have suffered as a result of DoubleClick’s purported illegal conduct. ...

Procedural History

This case is a multidistrict consolidated class action. The initial complaint was filed in this Court on January 31, 2000. On May 10, 2000, this Court consolidated the set of related federal class actions against DoubleClick in the Southern and
Eastern Districts of New York pursuant to Rule 42(a) of the Fed.R.Civ.P. and Local Rule 1.6 of the Southern and Eastern Districts of New York. ...

**BACKGROUND**

DoubleClick, a Delaware corporation, is the largest provider of Internet advertising products and services in the world. Its Internet-based advertising network of over 11,000 Web publishers has enabled DoubleClick to become the market leader in delivering online advertising. DoubleClick specializes in collecting, compiling and analyzing information about Internet users through proprietary technologies and techniques, and using it to target online advertising. DoubleClick has placed billions of advertisements on its clients’ behalf and its services reach the majority of Internet users in the United States. ...

**DoubleClick’s Technology and Services**

DoubleClick provides the Internet’s largest advertising service. Commercial Web sites often rent-out online advertising “space” to other Web sites. In the simplest type of arrangement, the host Web site (e.g., Lycos.com) rents space on its web-pages to another Web site (e.g., The-Globe.com) to place a “hotlink” banner advertisement (“banner advertisement”). When a user on the host Web site “clicks” on the banner advertisement, he is automatically connected to the advertiser's designated Web site.

DoubleClick acts as an intermediary between host Web sites and Web sites seeking to place banner advertisements. It promises client Web sites that it will place their banner advertisements in front of viewers who match their demographic target. For example, DoubleClick might try to place banner advertisements for a Web site that sells golf clubs in front of high-income people who follow golf and have a track record of making expensive online purchases. DoubleClick creates value for its customers in large part by building detailed profiles of Internet users and using them to target clients’ advertisements. ...

When users visit any of these DoubleClick-affiliated Web sites, a “cookie” is placed on their hard drives. Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner. However, Plaintiffs allege that DoubleClick’s cookies collect “information that Web users, including plaintiffs and the Class, consider to be personal and private, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect.” DoubleClick’s cookies store this personal information on users’ hard drives until DoubleClick electronically accesses the cookies and uploads the data.

How DoubleClick targets banner advertisements and utilizes cookies to collect user information is crucial to our analysis under the three statutes. Therefore, we examine both processes in greater detail.

**A. Targeting Banner Advertisements**

DoubleClick’s advertising targeting process involves three participants and four steps. The three participants are: (1) the user; (2) the DoubleClick-affiliated Web site; (3) the DoubleClick server. For the purposes of this discussion, we assume that a DoubleClick cookie already sits on the user’s computer with the identification number “# 0001.”
In Step One, a user seeks to access a DoubleClick-affiliated Web site such as Lycos.com. The user's browser sends a communication to Lycos.com (technically, to Lycos.com's server) saying, in essence, “Send me your homepage.” This communication may contain data submitted as part of the request, such as a query string or field information.

In Step Two, Lycos.com receives the request, processes it, and returns a communication to the user saying “Here is the Web page you requested.” The communication has two parts. The first part is a copy of the Lycos.com homepage, essentially the collection article summaries, pictures and hotlinks a user sees on his screen when Lycos.com appears. The only objects missing are the banner advertisements; in their places lie blank spaces. The second part of the communication is an IP-address link to the DoubleClick server. This link instructs the user's computer to send a communication automatically to DoubleClick’s server.

In Step Three, as per the IP-address instruction, the user's computer sends a communication to the DoubleClick server saying “I am cookie # 0001, send me banner advertisements to fill the blank spaces in the Lycos.com Web page.” This communication contains information including the cookie identification number, the name of the DoubleClick-affiliated Web site the user requested, and the user's browsertype.

Finally, in Step Four, the DoubleClick server identifies the user’s profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user's profile, to determine which advertisements it will present to the user. It then sends a communication to the user with banner advertisements saying “Here are the targeted banner advertisements for the Lycos.com homepage.” Meanwhile, it also updates the user's profile with the information from the request.

DoubleClick’s targeted advertising process is invisible to the user. His experience consists simply of requesting the Lycos.com homepage and, several moments later, receiving it complete with banner advertisements.

B. Cookie Information Collection

DoubleClick’s cookies only collect information from one step of the above process: Step One. The cookies capture certain parts of the communications that users send to DoubleClick-affiliated Web sites. They collect this information in three ways: (1) “GET” submissions, (2) “POST” submissions, and (3) “GIF” submissions.

GET information is submitted as part of a Web site's address or “URL,” in what is known as a “query string.” For example, a request for a hypothetical online record store's selection of Bon Jovi albums might read: http://recordstore.hypothetical.com/search?terms=bonjovi. The URL query string begins with the “?” character meaning the cookie would record that the user requested information about Bon Jovi.

Users submit POST information when they fill-in multiple blank fields on a web-page. For example, if a user signed-up for an online discussion group, he might have to fill-in fields with his name, address, email address, phone number and discussion group alias. The cookie would capture this submitted POST information.

Finally, DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users’ movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed.
Although the information collected by DoubleClick's cookies is allegedly voluminous and detailed, it is important to note three clearly defined parameters. First, DoubleClick's cookies only collect information concerning users' activities on DoubleClick-affiliated Web sites. Thus, if a user visits an unaffiliated Web site, the DoubleClick cookie captures no information. Second, plaintiff does not allege that DoubleClick ever attempted to collect any information other than the GET, POST, and GIF information submitted by users. DoubleClick is never alleged to have accessed files, programs or other information on users' hard drives. Third, DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking. As plaintiffs' counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an “opt-out” cookie; and (2) configuring their browsers to block any cookies from being deposited.

Once DoubleClick collects information from the cookies on users' hard drives, it aggregates and compiles the information to build demographic profiles of users. Plaintiffs allege that DoubleClick has more than 100 million user profiles in its database. Exploiting its proprietary Dynamic Advertising Reporting & Targeting (“DART”) technology, DoubleClick and its licensees target banner advertisements using these demographic profiles.

**DISCUSSION ...**

**CLAIM I. TITLE II OF THE ECPA**

Title II (“Title II”) of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §2701 et seq. (“§ 2701”), aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications. It creates both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission. Title II specifically defines the relevant prohibited conduct as follows:

(a) **Offense.** – Except as provided in subsection (c) of this section whoever(1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains ... access to a wire or electronic communication while it is in electronic storage in such system shall be punished. . . .

Plaintiffs contend that DoubleClick's placement of cookies on plaintiffs’ hard drives constitutes unauthorized access and, as a result, DoubleClick's collection of information from the cookies violates Title II. However, Title II contains an exception to its general prohibition.

(c) **Exceptions.** – Subsection (a) of this section does not apply with respect to conduct authorized... (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user;

DoubleClick argues that its conduct falls under this exception. It contends that the DoubleClick-affiliated Web sites are “users” of the Internet and that all of plaintiffs' communications accessed by DoubleClick's cookies have been “of or intended for” these Web sites. Therefore, it asserts, the Web sites' authorization excepts DoubleClick's access from § 2701(a)'s general prohibition. ...
C. All of the communications DoubleClick has accessed through its cookies have been authorized or have fallen outside of Title II’s scope. Because plaintiffs only allege that DoubleClick accessed communications from plaintiffs to DoubleClick-affiliated Web sites, the issue becomes whether the Web sites gave DoubleClick adequate authorization under § 2701(c)(2) to access those communications. This issue, in turn, has two parts: (1) have the DoubleClick-affiliated Web sites authorized DoubleClick to access plaintiffs’ communications to them?; and (2) is that authorization sufficient under § 2701(c)(2)?

1. The DoubleClick-affiliated Web sites have consented to DoubleClick’s interception of plaintiffs’ communications. ... Examining DoubleClick’s technological and commercial relationships with its affiliated Web sites, we find it implausible to infer that the Web sites have not authorized DoubleClick’s access. In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users’ demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs’ travels across the Web. However, that knowledge is irrelevant to the authorization at issue – Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs’ communications to them. As described in the earlier section “Targeting Banner Advertisements,” the DoubleClick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick’s access. This purely theoretical possibility that a DoubleClick-affiliated Web site might have been so ignorant as to have been unaware of the defining characteristic of DoubleClick’s advertising service – the service the Web site knowingly and purposely purchased – and its own role in facilitating that service, is too remote to be the basis for extensive and costly discovery of DoubleClick and its affiliates. Therefore, we find that the DoubleClick-affiliated Web sites consented to DoubleClick’s access of plaintiffs’ communications to them.

2. DoubleClick is authorized to access plaintiffs’ GET, POST and GIF submissions to the DoubleClick-affiliated Web sites. Plaintiffs’ GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all “intended for” those Web sites. In the case of the GET and POST submissions, users voluntarily type-in information they wish to submit to the Web sites, information such as queries, commercial orders, and personal information. GIF information is generated and collected when users use their computer “mouse” or other instruments to navigate through Web pages and access information. Although the users’ requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs’ GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all “intended for” those Web sites, the Web sites’ authorization is sufficient to except DoubleClick’s access under § 2701(c)(2). . . .
3. To the extent that the DoubleClick cookies’ identification numbers are electronic communications, (1) they fall outside of Title II’s scope, and (2) DoubleClick’s access to them is otherwise authorized. ... (b) If the DoubleClick cookies’ identification numbers are considered stored electronic communications, they are “of or intended for” DoubleClick and DoubleClick’s acquisition of them does not violate Title II.

Even if we were to assume that cookies and their identification numbers were “electronic communication[s] . . . in electronic storage,” DoubleClick’s access is still authorized. Section 2701(c)(2) excepts from Title II’s prohibition access, authorized by a “user,” to communications (1) “of” (2) “or intended for” that user. In every practical sense, the cookies’ identification numbers are internal DoubleClick communications – ” both “of” and “intended for” DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs’ hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers, that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick’s operations.

In this sense, cookie identification numbers are much akin to computer bar-codes or identification numbers placed on “business reply cards” found in magazines. These bar-codes and identification numbers are meaningless to consumers, but are valuable to companies in compiling data on consumer responses (e.g. from which magazine did the consumer get the card?). Although consumers fill-out business reply cards and return them to companies by mail, the bar-codes and identification numbers that appear on the cards are purely internal administrative data for the companies. The cookie identification numbers are every bit as internal to DoubleClick as the bar-codes and identification numbers are to business reply mailers. Therefore, it seems both sensible to consider the identification numbers to be “of or intended for” DoubleClick and bizarre to describe them as “of or intended for” plaintiffs. Accordingly, because the identification numbers are “of or intended for” DoubleClick, it does not violate Title II for DoubleClick to obtain them from plaintiffs’ electronic storage.

To summarize, plaintiffs’ GET, POST and GIF submissions are excepted from § 2701(c)(2) because they are “intended for” the DoubleClick-affiliated Web sites who have authorized DoubleClick’s access. The cookie identification numbers sent to DoubleClick from plaintiffs’ computers fall outside of Title II’s protection because they are not in “electronic storage” and, even if they were, DoubleClick is authorized to access its own communications.

In light of the above findings, we rule that all of plaintiffs’ communications accessed by DoubleClick fall under § 2701(c)(2)’s exception or outside Title II and, accordingly, are not actionable. Therefore, plaintiffs’ claim under the Title II (Claim I) is dismissed.

Claim II. Wiretap Act

[The court rejected the plaintiffs’ Wiretap Act claim because it held that the affiliated websites were “parties” to the communication and consented to DoubleClick’s actions.]
QUESTIONS

1. Cookies were originally designed to allow users to log in to web sites and have the sites remember them later. The web site “sets a cookie” when you log in; later, it “retrieves” the cookie and recognizes you. Companies like DoubleClick figured out how to use this technology to serve personalized ads. The court’s discussion of how cookies work is a bit dry. Can you do better? Draw a picture: what information is transmitted to whom, and when?

2. DoubleClick holds that DoubleClick’s use of cookies violated neither the SCA nor the Wiretap Act. Why? Are you convinced by the court’s reading of the statutes? Once you draw the pictures, do cookies seem more or less like a form of worrisome surveillance? Is the harm here a harm of the sort these laws were intended to prevent?

3. Or is it not a harm at all? Ad networks like DoubleClick have always said that they offer consumers a useful service. What service is that? How useful do you find it? How would the Web change if DoubleClick-style tracking cookies were banned tomorrow? Which forms of web advertising do you find most annoying? Creepiest? Which, if any, would you prohibit?

4. DoubleClick (now owned by Google) offers an opt-out from its cookie tracking at http://www.google.com/privacy/ads/. The fraction of Internet users who have opted out it is infinitesimal. Why might that be? Does the fact that most users haven’t opted out indicate that they don’t care about personal privacy of this sort? Would an opt-in system be better?

IN RE GOOGLE, INC. PRIVACY POLICY LITIG.

Grewal, Magistrate Judge:

After this court’s order dismissing their consolidated complaint on standing grounds with leave to amend, Plaintiffs Robert Demars, Pedro Marti, David Nisenbaum, Lorena Barrios, Nicholas Anderson, Matthew Villani and Scott McCullough (“Plaintiffs”) filed an amended complaint. In their amended complaint, Plaintiffs again challenge the introduction of a new, unified privacy policy by Defendant Google, Inc. (“Google”) permitting the commingling of user data across different Google products. Plaintiffs also challenge Google’s disclosure of this data to third parties, including developers of applications for the Google Play market and advertising partners. Google again moves to dismiss, arguing that Plaintiffs still lack standing because they have not sufficiently alleged any injury-in-fact traceable to Google. Google also argues that Plaintiffs have failed to state any claim upon which relief may be granted. As detailed below, the court agrees with Google that the amended complaint is defective and therefore must be dismissed, but only in part and with further leave to amend.

I. Background

By now, most people know who Google is and what Google does. Google serves billions of online users in this country and around the world. What started as simply a search engine has expanded to many other products such as YouTube and Gmail. Google offers these products and most others without charge. With little or no revenue from its users, Google still manages to turn a healthy profit by selling advertisements within its products that rely in substantial part on users’ personal identification information (“PII”). As some before have observed, in this model, the users are the real product.
Before March 1, 2012, Google maintained separate privacy policies for each of its products, each of which confirmed that Google used a user's PII to provide that particular product. These policies also confirmed that Google would not use the PII for any other purpose without the user's explicit consent. As Google put it, “when you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.”

On March 1, 2012, Google announced a new policy. The majority of its separate privacy policies were eliminated in favor of a single, universal privacy policy that spells out that Google may combine a user’s PII across multiple Google products. Google explained the basis for the change in policy as follows:

Our new Privacy Policy makes clear that, if you’re signed in, we may combine information that you’ve provided from one service with information from other services. In short, we’ll treat you as a single user across all our products, which will mean simpler, more intuitive Google experience.

In other words, through the new policy, Google is explicit that it may combine PII collected from a user’s Gmail or YouTube account, including the content of that account, with PII collected from that user’s Google search queries, along with the user’s activities on other Google products, such as Picasa, Maps, Docs, and Reader. This PII includes:

- first and last name;
- home or other physical address (including street name and city);
- current, physical location, a user’s email address, and other online contact information (such as the identifier or screen name);
- IP address;
- telephone number (both home and mobile numbers);
- list of contacts;
- search history from Google’s search engine;
- web surfing history from cookies placed on the computer; and
- posts on Google+.

Plaintiffs contend that Google’s new policy violates its prior policies because the new policy no longer allows users to keep information gathered from one Google product separate from information gathered from other Google products. Plaintiffs further contend that Google’s new policy violates users’ privacy rights by allowing Google to take information from a user’s Gmail account, for which users may have one expectation of privacy, for use in a different context, such as to personalize Google search engine results, or to personalize advertisements shown while a user is surfing the internet, products for which a user may have an entirely different expectation of privacy. In addition to commingling Plaintiffs’ PII across

---

3 For example, in a legal notice issued to Gmail users in 2011, Google stated, “We will not use any of your content [defined to include ‘text, data, information, images, photographs, music, sound, video, or other material’] for any purpose except to provide you with the service.” Google has also pledged that “Gmail stores processes, and maintains your messages, contact lists, and other data related to your account in order to provide the service to you.”
the various Google products, Plaintiff contend Google has shared Plaintiffs’ PII with third-party entities who have partnered with Google in order to develop applications for the Google Play app store to help it place targeted advertisements.

Plaintiffs bring this nationwide class action against Google on behalf of all persons and entities in the United States who acquired a Google account between August 19, 2004, and February 29, 2012, and maintained such an account until, on, or after March 1, 2012. Plaintiffs also bring this action on behalf of [two subclasses of purchasers of Android phones].

Plaintiffs allege that they each acquired a Gmail account before the March 1, 2012 announcement of the new policy and continued to use it after the new policy took effect. They each further allege they purchased an Android phone before March 1 and that after implementing the new policy Google aggregated their personal information without consent or compensation. Mr. Marti further alleges Google used his likeness in display advertisements without authorization. Mr. Nisenbaum further alleges that after March 1, for privacy reasons, he replaced his Android phone for privacy reasons with an iPhone. The other plaintiffs allege use of various Android-powered phones and that they downloaded various Android Applications (“apps”) from the Google Play store. Based on these allegations, Plaintiffs bring claims against Google for statutory and common law misappropriation of likeness, violation of California’s Unfair Competition Law (“UCL”), breach of contract, common law intrusion upon seclusion, violation of California’s User Legal Remedies Act (“CLRA”), violation of the Wiretap Act, and violation of the Stored Communications Act (“SCA”).

II. LEGAL STANDARDS

To satisfy Article III, a plaintiff “must show that (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” See Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc., 528 U.S. 167, 180–181 (2000). A suit brought by a plaintiff without Article III standing is not a “case or controversy,” and an Article III court therefore lacks subject matter jurisdiction over the suit. In that event, the suit should be dismissed under Fed. R. Civ. Pro. 12(b)(1). ...

[The court recited the usual pleading standards to survive a Rule 12(b)(6) motion to dismiss for failure to state a claim – a “short plain statement of the claim showing that the pleader is entitled to relief” – and the heightened pleading standards of Rule 9(b) for claims sounding in fraud or mistake – “pleading with particularity the circumstances surrounding the fraud or mistake.”]

Dismissal with prejudice and without leave to amend is not appropriate unless it is clear that the complaint could not be saved by amendment. A dismissal with prejudice, except one for lack of jurisdiction, improper venue, or failure to join a party operates as an adjudication on the merits. Dismissal without leave to amend, however, may be granted for reasons of undue delay, bad faith, repeated failure to cure deficiencies by previous amendments, futility of the amendment, and prejudice.

III. DISCUSSION

A. Article III Standing ...

Plaintiffs aim to establish their standing with six theories of injury that can fairly be grouped into three categories: (1) commingling of Plaintiffs’ PII, (2) direct eco-
nomic injury, and (3) violations of statutorily created rights. The court considers each category in turn.

1. **Personal Identification Information**

Plaintiffs claim that when Google combined information that Plaintiffs provided to discrete Google products, without Plaintiffs’ consent, Google injured them in two different ways. First, Google did not compensate them for the substantial economic value of the combined information. Second, Google’s unauthorized commingling of their information, especially their likeness, was a breach of contract. Neither alleged harm, however, is sufficient to establish an injury-in-fact.

As the court previously explained, injury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff’s personal identification information. Rather, a plaintiff must allege how the defendant’s use of the information deprived the plaintiff of the information’s economic value. Put another way, a plaintiff must do more than point to the dollars in a defendant’s pocket; he must sufficient allege that in the process he lost dollars of his own. Plaintiffs’ allegations certainly plead that Google made money using information about them for which they were provided no compensation beyond free access to Google’s services. But an allegation that Google profited is not enough equivalent to an allegation that such profiteering deprived Plaintiffs’ of economic value from that same information.

As before, the court finds the reasoning in *LaCourt v. Specific Media*, No. SACV 10–1256–GW (JCGX), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), instructive. There the plaintiffs alleged that the defendant installed cookies to track users’ internet browsing to build behavior profiles to better target advertisements. The court found the tracked users lacked standing because, among other reasons, they did not “explain how they were ‘deprived’ of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party.” ...

Finally, although Plaintiffs assert that the breach of contract arising from Google’s unauthorized commingling activities offers a separate basis for injury-in-fact, they still fail to articulate a sufficient contract injury. Nominal damages are not available in California for breach of contract, and the amended complaint does not allege any other injury based on the breach. ... This is insufficient.

2. **Direct Economic Injuries**

The court next considers whether Plaintiffs have alleged direct economic injuries sufficient to establish injury-in-fact. As the Supreme Court has noted, palpable economic injuries have long been recognized as sufficient to lay the basis for standing. Plaintiffs each allege that they were injured when their Android devices sent their respective names, email addresses, and locations to the developer of each app they purchased or downloaded because they had to pay for the battery and bandwidth consumed by the unauthorized transmissions. Mr. Nisenbaum, representing the Android Device Switch Subclass, claims further injury in that he overpaid for his Android phone in 2010 because he would not have bought the phone had Google disclosed its intention to use his information as alleged in the complaint. Mr. Nisenbaum also claims that he replaced his Android phone with an iPhone in 2012 as a result of Google’s policy change, causing him further economic injury.
The Court will consider each of these direct economic injury theories in turn to
determine if they articulate “something more” than pure economic harm to sup-
port subject-matter jurisdiction under Rule 12(b)(1).

With respect to Plaintiffs’ injury claims based on battery and bandwidth con-
sumption, courts have found that the unauthorized use of system resources can
suffice to establish a cognizable injury. For example, in Goodman v. HTC America,
found standing based upon battery discharge where the application at issue sent
fine location data every three hours or whenever the device’s screen was refreshed.
Similarly, in In re iPhone Application Litigation, No. 5:11–md–02250–LHK, 2011
WL 4403963 (N.D. Cal. Sept. 20, 2011), the court found standing where the de-
vice systematically collected and transmitted location information. In In re Google
Android User Privacy Litig., No. 5:11–md–02264–JSW, 2013 WL 1283236 (N.D.
Cal. Mar. 26, 2013), the plaintiffs did not clearly allege how frequently Google col-
glected geolocation data from a phone, but did allege that collecting relocation data
was particularly battery intensive, that “their batteries discharged more quickly[,] and
that their services were interrupted.” This latter allegation was deemed suffi-
cient to establish standing. At the same time, in Hernandez v. Path, Inc., No. 12–
CV–01515 YGR, 2012 WL 5194120 (N.D. Cal. Oct. 19, 2012), the court found that
any harm from the use of phone resources in an app’s uploading a user’s address
book a single time upon first running the app was de minimis and thus insufficient
to establish injury.

Plaintiffs’ allegations here are closer to Goodman, iPhone I and Android than
Hernandez. Like Hernandez, Plaintiffs’ alleged unauthorized battery consumption
only happened infrequently, when a plaintiff first downloaded an app. But in Her-
nandez the allegedly unauthorized upload only happened once, when a plaintiff
downloaded the Path app. Here, it happens each time a user downloads any app.
The plaintiff who downloaded the most apps, according to the amended com-
plaint, did so at least 27 times. In addition, like the plaintiffs in Goodman and An-
droid, Plaintiffs here specifically allege a greater discharge of battery power as a
result of unauthorized conduct and as in iPhone I the discharge is systemic rather
than episodic. This is sufficient to establish more than a de minimis injury.

With respect to Mr. Nisenbaum’s further allegations of injury, they, too, support
standing for purposes of Article III.

First, the allegation that Mr. Nisenbaum bought a new phone after the policy
change and that his motivation for choosing an iPhone over the Android device
was substantially for privacy reasons, establishes that he was injured by making
the purchase. To be sure, users frequently replace old phones for all kinds of rea-
sons beyond privacy. For example, from the complaint, it appears Mr. Nisenbaum
had his Android device for approximately two years, the length of most phone con-
tracts that often include a discount for bundled phones, before purchasing a new
phone. But Mr. Nisenbaum specifically alleges that but for the policy switch he
would not have otherwise bought a new phone. The alleged injury is fairly
traceable to Google based on Mr. Nisenbaum’s allegation that he relied on Google’s
previous policies in purchasing the Android phone in the first place.

Second, Mr. Nisenbaum’s allegations regarding overpayment establish injury.

3. Violation of Statutory Rights
The final category of Plaintiffs’ injury-in-fact theories concerns statutory rights.
The Ninth Circuit has made it clear that Article III standing can also be estab-
lished by virtue of “statutes creating legal rights, the invasion of which creates standing. Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010). ... To decide if a statute created such a legal right, a court must determine whether the “standing provision on which the claim rests properly can be understood as granting persons in the plaintiff’s position a right to judicial relief.” Id. ... Although Article III always requires an injury, the alleged violation of a statutory right that does not otherwise require a showing of damages is an injury sufficient to establish Article III standing. For example, in a case where a credit card company failed to make required disclosures and the Truth in Lending Act created a private right of action for such failures without a showing of damages, the Ninth Circuit held that the plaintiff “suffered the loss of a statutory right to disclosure and has therefore suffered injury in fact for purposes of Article III standing.” DeMando v. Morris, 206 F.3d 1300, 1303 (9th Cir. 2000). ... 

Plaintiffs have alleged unauthorized access and wrongful disclosure of communications, including disclosure to third parties. Plaintiffs also have alleged the interception of communications. Courts have recognized that such alleged violations of the Wiretap Act or the Stored Communications Act are sufficient to establish Article III injury. These statutes grant persons in Plaintiffs’ position a right to relief and thus Plaintiffs have standing for these claims.

The complaint also alleges that Mr. Marti was injured when Google used his name or likeness in connection with its “+1” function without authorization. California Civil Code Section 3344 prohibits the commercial use another’s name or likeness. The statute thus creates a right of action for “persons injured as a result thereof.” ...

Google disputes any injury-in-fact from the +1 feature because Plaintiffs have not alleged an unauthorized use. However, the amended complaint states that Google did not compensate Mr. Marti for the commercial use of his personal endorsement and that he “did not authorize Google’s use of that endorsement.” As explained above, whatever the merits of the parties’ competing views of consent, a merits analysis is not appropriate when considering standing. ...

B. [Wiretap Act] ...

The Wiretap Act, as amended by the Electronic Communication Privacy Act (“ECPA”), generally prohibits the intentional interception of “wire, oral, or electronic communications.” 18 U.S.C. § 2511(1). The purpose of the Wiretap Act is to protect the privacy of communications. ... The Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Id. § 2510(4). However, the definition of “electronic, mechanical, or other device” excludes [any instrument “being used by a provider of wire or electronic communication service in the ordinary course of its business.” Id. § 2510(5)(a)(ii)].

The amended complaint fails to allege any interception by Google that falls outside the scope of this broad immunity. While Plaintiffs point to their allegations that Google’s use of the accused devices to intercept Gmail communications and co-mingle the contents and distribute those contents without consent was not necessary to the delivery of Gmail, this narrow read of the exemption, as being limited to only action taken to deliver the electronic communication, does not square with the plain meaning of the statutory text at issue. The text exempts from the definition of “intercept” any use of a device by a provider “in the ordinary course of its business.” Rather than narrowing the exemption to only the provision of electronic communications services itself, or some such narrower scope, Con-
gress specifically chose the broader term “business” that covers more far-ranging activity. For good measure, Congress also teamed the term “business” with the terms “ordinary course,” suggesting an interest in protecting a provider’s customary and routine business practices. ...

Although the Ninth Circuit has yet to rule on the subject, other appellate courts that have agreed that the “ordinary course of business” exception is not limited to actions necessary to providing the electronic communication services (“ECS”) at issue. ... In *Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1250 (10th Cir. 2012), the Tenth Circuit held that the defendant was protected by the exception when it conducted a test using third-party advertising technology and its customers’ communications, because the defendant had “no more of its users’ electronic communications than it had in the ordinary course of its business as an ISP.” The trial court’s decision affirmed by *Kirch* noted that the “ordinary course of its business” defense “appears to have merit, as plaintiffs have admitted that Embarq conducted the NebuAd test to further legitimate business purposes and that behavioral advertising is a widespread business and is commonplace on the Internet.” *Kirch*, No. 10–2047–JAR, 2011 WL 3651359, at *9 n.42 (D. Kan. Aug. 19, 2011). *Kirch* thus supports the application of Section 2510(5)(a)(ii) where the provider is furthering its “legitimate business purposes” – including advertising – and is not limited to only those acts that are technically necessary to processing email.

The more fundamental problem with Plaintiffs’ narrow construction of Section 2510(5)(a)(ii) is that in defining “ordinary course of business” as “necessary” it begs the question of what exactly its means for a given action to be “necessary” to the delivery of Gmail. For example, in delivering Gmail is it really “necessary” do more than just the comply with email protocols such as POP, IMAP and MAPI? What about spam-filtering or indexing? None of these activities have anything specifically to do with transmitting email. And yet not even Plaintiffs suggest that these activities are unnecessary and thus lie outside of the “ordinary course business.” ...

C. Stored Communications Act

The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. Despite this purpose, the SCA has a narrow scope: the SCA is not a catch-all statute designed to protect the privacy of stored Internet communications.

Plaintiffs claim that Google violated the SCA in two ways. First, they claim that in aggregating users’ information between Google services without their consent, Google exceeded the scope of Google’s authorized access in violation of 18 U.S.C. § 2701(a). This claim borders on frivolous, considering the plain language of subsection (c) of Section 2701(a) that exempts conduct authorized “by the person or entity providing a wire or electronic communications service.” Whatever the propriety of Google’s actions, it plainly authorized actions that it took itself.

Second, Plaintiffs claim that Google shared stored communications with third parties in violation of Section 2702(a). Section 2702(a) prohibits providers of electronic communication services from “knowingly divulging] to any person or entity the contents of a communication....” Plaintiffs’ only allegation supporting its second theory is that:

insofar as Google engages independent, unidentified third-party entities to process and distribute user information across its product platforms, including the contents of Plaintiffs’ Gmail communications,
Google intentionally discloses the contents of those communications outside of Google.

But “insofar” is not a concrete allegation; it is theoretical and does not support a claim. Even if this were a concrete allegation, it is too conclusory to support a claim. Plaintiffs simply fail to state any claim under the SCA.

D. Misappropriation of Likeness

California Civil Code Section 3344 prohibits the use of another’s name or likeness [“to defendant’s advantage, commercially or otherwise”] without the person’s consent. ... Here, Plaintiffs fail to adequately allege lack of consent. ...

Plaintiffs in this case only make a threadbare allegation that Google did not obtain their consent to use their name or likeness in advertisements associated with its “+1” feature, and the claim is not supported by other allegations. To the contrary, the complaint alleges that Ms. Marti voluntarily clicked on the “+1” feature, that Google clearly disclosed how the feature worked as part of the feature’s launch, and that the feature worked as Google said it would when Marti used it. In particular, the amended complaint quotes Google as: describing the “+1” feature as “the digital shorthand for ‘this is pretty cool’” and a way “to share recommendations with the world;” explaining that to “[t]o recommend something, all you have to do is click +1 on a webpage or ad you find useful;” and giving the example of a person planning a winter trip to Tahoe, California who, when doing a search, “may now see a +1 from [his] slalom-skiing aunt next to the result for a lodge in the area.”

Without some contradictory allegations, this is a clear disclosure of how the feature worked such that the voluntary use of it constituted consent. Plaintiffs therefore have not stated any claim for statutory or common law misappropriation of likeness.

E. Breach of Contract ...

Google argues that it has not breached its contact with Plaintiffs because the original contract included provisions for it to make the types of very changes that Plaintiffs allege breached the contract. ...

The policy plainly includes a provision for the commingling of PII across Google products. That provision states: “We may combine the information you submit under your account with information from other services.” In light of this express provision, it is not plausible to say that Google could be considered to have breached the contract. Plaintiffs again have failed to state a claim.

F. California’s Unfair Competition Law (“UCL”)

California’s UCL provides a private cause of action for users who are harmed by unfair, unlawful, or fraudulent business practices. Plaintiffs here plead their UCL claim under all three prongs. To sustain a claim under the unlawful prong, Plaintiffs must allege facts that, if proven, would demonstrate that Defendant’s conduct violated another, underlying law. ... Under the fraudulent prong, Plaintiffs must allege specific facts to show that the members of the public are likely to be deceived by the actions of the defendant. The Ninth Circuit has established that this

113 For example, Plaintiffs might have a claim if they could allege that the feature did not work as Google explained, that Google did not adequately disclose how the feature worked, a theory of how clicking on the “+1” feature did not demonstrate consent, or an allegation that his name or likeness was associated with brands, products, or websites he did not “+1.”
prong is subject to Fed. Rule Civ. P. 9(b)’s heightened pleading requirements. With respect to Plaintiffs’ final claim under the UCL’s unfair prong, the standard for determining what business acts or practices are “unfair” in user actions under the UCL is currently unsettled. Generally speaking, an unfair business practice under the UCL is “one that either offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to users.” *McDonald v. Coldwell Banker*, 543 F.3d 498, 506 (9th Cir. 2008). To determine whether a business practice is unfair, a court should consider “the impact of the practice or act on its victim, balanced against the reasons, justifications and motives of the alleged wrongdoer;” this prong of the UCL should be used to enjoin deceptive or sharp practices.” *Wilson v. Hynek*, 207 Cal. App. 4th 999, 1008 (Cal. Ct. App. 2012).

To support their claim under the UCL’s unlawful prong, Plaintiffs allege that Google’s conduct violates [the laws discussed above]. As discussed in other sections, Plaintiffs have failed to set forth sufficient factual allegations to support these underlying charges, and without having plead any underlying unlawful conduct, Plaintiffs unlawful conduct claim under the UCL must be dismissed.

With respect to their claim under the fraudulent prong, Plaintiffs allege that when Google collected their PII before March 1, 2012, it assured them that it would not use the information for any purpose other than delivering the service for which the users provided it. [But] the documents submitted for judicial notice undermine any notion that Google failed to disclose its data commingling practices before March 1, 2012.

Finally, Plaintiffs seek to support their claim of unfair conduct by alleging that Google lead them to believe that they could opt out of endorsements, profiting from the use of the plaintiff’s information, and “encouraging Plaintiffs and the Class to make Google products indispensable to their lives,” before making it incredibly difficult for them to effectively “opt out” of programs making use of their data. These facts, as alleged, do not rise to the level of “unscrupulous” or “unethical.” Even if its earlier policies were not transparent, Google provided notice to its users when it changed its privacy policy, which undercuts any unethical or immoral allegations; this was not a change made in the dark, but rather one broadcast to all those affected. In addition, the overall benefit to users in receiving free, “indispensable” services offsets much of the harm they may suffer through the change. As it stands, Plaintiffs have not set forth sufficient allegations to support an unfairness prong claim.

**G. Common Law Intrusion Upon Seclusion**

In order to put forth a claim for intrusion upon seclusion, a plaintiff must plead facts to support two elements: 1) intrusion into a private place, conversation or matter, and 2) in a manner highly offensive to a reasonable person. To show intrusion, a plaintiff must have an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source, and the defendant must have ‘penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff. ... In this context, the concept of ‘seclusion’ is relative. The mere fact that a person or their information can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone. Courts have recognized facts sufficient to support these elements in the context of repeated phone calls, eavesdropping on workplace conversations, and unauthorized review of email.
Plaintiffs here allege that Google’s PII commingling intruded upon their email, contact lists, web histories, and other secluded and private spaces. According to Plaintiffs, this expectation was reasonable in light of the previous privacy policies, which assured Plaintiffs of the isolated use of their data. But once again, the court does not find any expectation to be plausible in light of Google’s earlier disclosure that it would commingle PII across products to support its advertising model. Without a plausible expectation, Plaintiffs’ seclusion on intrusion claim cannot stand.

H. California’s User Legal Remedies Act (“CLRA”)

Plaintiffs’ sixth cause of action seeks recovery under Sections (a)(9), (14), and (16) of the CLRA, which ban advertising goods with intent not to sell them in the manner advertised, representing that a transaction conveys rights which it does not, and representing that the subject of a transaction has been conveyed in accordance with terms of a previous transaction, when it has not. In order to recover, Plaintiffs must also allege facts to establish that they relied on the misrepresentations in question, and that in so relying, they suffered damage. These allegations are subject to Rule 9(b)’s heightened pleading standards.

Plaintiffs’ claims are insufficiently plead because they fail to allege that Google intended to use the PII in a manner other was advertised at the time that the plaintiffs purchased the goods and registered for the services in question. Under the CLRA, the intent to deceive or misuse information must be present at the time of sale in order for a plaintiff to recover. Yet even if its commingling practices were not disclosed in 2010, Plaintiffs offer no factual allegations indicating that Google planned to change its policies as far back as 2010, such that the existing policies were aimed to deceive at the time the business relationship began. They have not put forth any allegations suggesting that Google did not intend to honor its existing privacy policies, at the time they became customers. They certainly do not provide the requisite level of detail under Rule 9(b) to support allegations of intent to deceive.

IV. Conclusion

Google’s motion to dismiss is GRANTED. Plaintiffs must file any further amended complaint by January 16, 2014. Having dismissed two complaints already, Plaintiffs are on notice that any further dismissal will likely be with prejudice.

QUESTIONS

1. Why is it so hard for the plaintiffs to plead injury? Is their problem that they haven’t actually been injured, or that the legal system doesn’t care about privacy harms?
2. Loss of battery life? Seriously?
3. Suppose that the defendant suffers a data breach that exposes plaintiffs’ names, addresses, phone numbers, email addresses, and dates of birth. Plaintiffs sue, alleging increased likelihood of identity theft. Have they suffered an injury in fact for standing purchases? What if they have had unauthorized purchases made using their credit cards, but are not financially responsible for those purchases under their credit-card agreements? Can they claim injury-in-fact based on the time and hassle involved in reversing the unauthorized charges?
4. Is the court right that Google’s earlier statements put plaintiffs on notice that it might commingle their data? If so, how much are privacy promises really worth?

IN RE SNAPCHAT, INC.
2015-1 Trade Cas. (CCH) ¶ 17,115, 2014 WL 7495798 (F.T.C. 2014)

COMPLAINT

The Federal Trade Commission, having reason to believe that Snapchat, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges: ...

Respondent’s Business Practices

3. Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as “snaps.” Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap. Snapchat markets the application as an “ephemeral” messaging application, having claimed that once the timer expires, the snap “disappears forever.”

4. Snapchat launched its mobile application on Apple Inc.’s iOS operating system in September 2011 and on Google Inc.’s Android operating system in October 2012. Snapchat added video messaging to the iOS version of its application in December 2012 and to the Android version of its application in February 2013.

5. Both the iTunes App Store and the Google Play store list Snapchat among the top 15 free applications. As of September 2013, users transmit more than 350 million snaps daily.

Snapchat's “Disappearing” Messages (Counts 1 and 2)

6. Snapchat marketed its application as a service for sending “disappearing” photo and video messages, declaring that the message sender “control[s] how long your friends can view your message.” Before sending a snap, the application requires the sender to designate a period of time - with the default set to a maximum of 10 seconds - that the recipient will be allowed to view the snap ...

7. Since the application’s launch on iOS until May 2013, and since the application’s launch on Android until June 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statements on its product description page on the iTunes App Store and Google Play:

8. From October 2012 to October 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statement on the “FAQ” page on its website:

   Is there any way to view an image after the time has expired?
   No, snaps disappear after the timer runs out ....

9. Despite these claims, several methods exist by which a recipient can use tools outside of the application to save both photo and video messages, allowing the recipient to access and view the photos or videos indefinitely.
10. For example, when a recipient receives a video message, the application stores the video file in a location outside of the application's "sandbox" (i.e., the application's private storage area on the device that other applications cannot access). Because the file is stored in this unrestricted area, until October 2013, a recipient could connect his or her mobile device to a computer and use simple file browsing tools to locate and save the video file. This method for saving video files sent through the application was widely publicized as early as December 2012. Snapchat did not mitigate this flaw until October 2013, when it began encrypting video files sent through the application.

11. Furthermore, third-party developers have built applications that can connect to Snapchat's application programming interface ("API"), thereby allowing recipients to log into the Snapchat service without using the official Snapchat application. Because the timer and related "deletion" functionality is dependent on the recipient's use of the official Snapchat application, recipients can instead simply use a third-party application to download and save both photo and video messages. As early as June 2012, a security researcher warned Snapchat that it would be "pretty easy to write a tool to download and save the images a user receives" due to the way the API functions. Indeed, beginning in spring 2013, third-party developers released several applications on the iTunes App Store and Google Play that recipients can use to save and view photo or video messages indefinitely. On Google Play alone, ten of these applications have been downloaded as many as 1.7 million times.

12. The file browsing tools and third-party applications described in paragraphs 10 and 11 are free or low cost and publicly available on the Internet. In order to download, install, and use these tools, a recipient need not make any modifications to the iOS or Android operating systems and would need little technical knowledge.
13. In addition to the methods described in paragraphs 10-12, a recipient can use the mobile device’s screenshot capability to capture an image of a snap while it appears on the device screen.

14. Snapchat claimed that if a recipient took a screenshot of a snap, the sender would be notified. On its product description pages, as described in paragraph 7, Snapchat stated: “We’ll let you know if [recipients] take a screenshot!” In addition, from October 2012 to February 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statement on the “FAQ” page on its website:

**What if I take a screenshot?**
Screenshots can be captured if you’re quick. The sender will be notified immediately.

15. However, recipients can easily circumvent Snapchat’s screenshot detection mechanism. For example, on versions of iOS prior to iOS 7, the recipient need only double press the device’s Home button in rapid succession to evade the detection mechanism and take a screenshot of any snap without the sender being notified. This method was widely publicized.

16. As described in Paragraphs 6, 7, and 8, Snapchat has represented, expressly or by implication, that when sending a message through its application, the message will disappear forever after the user-set time period expires.

17. In truth and in fact, as described in Paragraph 9-12, when sending a message through its application, the message may not disappear forever after the user-set time period expires. Therefore, the representation set forth in Paragraph 16 is false or misleading.

**Count 1**

18. As described in Paragraphs 7 and 14, Snapchat has represented, expressly or by implication, that the sender will be notified if the recipient takes a screenshot of a snap.

19. In truth and in fact, as described in Paragraph 15, the sender may not be notified if the recipient takes a screenshot of a snap. Therefore, the representation set forth in Paragraph 18 is false or misleading.

**Snapchat’s Collection of Geolocation Information (Count 3)**

20. From June 2011 to February 2013, Snapchat disseminated or caused to be disseminated to consumers the following statements in its privacy policy:

> We do not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application.

21. In October 2012, Snapchat integrated an analytics tracking service in the Android version of its application that acted as its service provider. While the Android operating system provided notice to consumers that the application may access location information, Snapchat did not disclose that it would, in fact, access location information, and continued to represent that Snapchat did “not ask for, track, or access any location-specific information ...”

22. Contrary to the representation in Snapchat’s privacy policy, from October 2012 to February 2013, the Snapchat application on Android transmitted
Wi-Fi-based and cell-based location information from users’ mobile devices to its analytics tracking service provider.

Count 3

23. As described in Paragraph 21, Snapchat has represented, expressly or by implication, that it does not collect users’ location information.

24. In truth and in fact, as described in Paragraph 22, Snapchat did collect users’ location information. Therefore, the representation set forth in Paragraph 23 is false or misleading. ...

Snapchat’s Collection of Contacts Information (Counts 4 and 5) ...  

25. Snapchat provides its users with a feature to find friends on the service. During registration, the application prompts the user to “Enter your mobile number to find your friends on Snapchat!,” implying - prior to September 2012 - through its user interface that the mobile phone number was the only information Snapchat collected to find the user’s friends, as depicted below: ...

26. However, when the user chooses to Find Friends, Snapchat collects not only the phone number a user enters, but also, without informing the user, the names and phone numbers of all the contacts in the user’s mobile device address book.

[The FTC alleged that the failure to notify users was false or misleading, and that Snapchat made deceptive statements in its privacy policy about the feature.]  

Snapchat’s Failure to Secure Its Find Friends Feature (Count 6) ...

35. From September 2011 to December 2012, Snapchat failed to verify that the phone number that an iOS user entered into the application did, in fact, belong to the mobile device being used by that individual. Due to this failure, an individual could create an account using a phone number that belonged to another consumer, enabling the individual to send and receive snaps associated with another consumer’s phone number.

36. Numerous consumers complained to Snapchat that individuals had created Snapchat accounts with phone numbers belonging to other consumers, leading to the misuse and unintentional disclosure of consumers’ personal information. For example, consumers complained that they had sent snaps to accounts under the belief that they were communicating with a friend, when in fact they were not, resulting in the unintentional disclosure of photos containing personal information. In addition, consumers
complained that accounts associated with their phone numbers had been used to send inappropriate or offensive snaps.

37. Snapchat could have prevented the misuse and unintentional disclosure of consumers’ personal information by verifying phone numbers using common and readily available methods.

38. Indeed, in December 2012, Snapchat began performing short-message-service (“SMS”) verification to confirm that the entered phone number did in fact belong to the mobile device being used by that individual.

39. In addition, from September 2011 to December 2013, Snapchat failed to implement effective restrictions on the number of Find Friend requests that any one account could make to its API. Furthermore, Snapchat failed to implement any restrictions on serial and automated account creation. As a result of these failures, in December 2013, attackers were able to use multiple accounts to send millions of Find Friend requests using randomly generated phone numbers. The attackers were able to compile a database of 4.6 million Snapchat usernames and the associated mobile phone numbers. The exposure of usernames and mobile phone numbers could lead to costly spam, phishing, and other unsolicited communications. ...

40. ... Snapchat disseminated or caused to be disseminated to consumers the following statement in its privacy policy:

   Snapchat takes reasonable steps to help protect your personal information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration, and destruction. ...

   **Count 6**

43. As described in Paragraphs 40–42, Snapchat has represented, expressly or by implication, that it employs reasonable security measures to protect personal information from misuse and unauthorized disclosure.

44. In truth and in fact, as described in Paragraphs 34–39, in many instances, Snapchat did not employ reasonable security measures to protect personal information from misuse and unauthorized disclosure. Therefore, the representation set forth in Paragraph 43 is false or misleading.

45. The acts and practices of respondent as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-third day of December, 2014, has issued this complaint against respondent.

**DECISION AND ORDER** ...

[Snapchat entered into a consent order under which it neither admitted nor denied the allegations in the complaint but agreed to certain changes in its business practices.]

**Definitions**

For purposes of this Order, the following definitions shall apply: ...

3. “Covered information” shall mean information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a
persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (f) precise geo-location data of an individual or mobile device, including GPS-based, Wi-Fi-based, or cell-based location information; (g) an authentication credential, such as a username or password; or (h) any communications or content that is transmitted or stored through respondent’s products or services.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, shall not misrepresent in any manner, expressly or by implication, in or affecting commerce, the extent to which respondent or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: (1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which respondent or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information.

II.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent’s products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain privacy controls and procedures appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information, including [designation of employees responsible for the privacy program, identification of foreseeable privacy risks, implementation of reasonable privacy controls to address those risks, appropriate security practices, and ongoing adjustment of the program in light of changing circumstances].

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional ...

VIII.

This order will terminate twenty (20) years from the date of its issuance ...

QUESTIONS

1. The FTC has the power to investigate and prohibit “unfair or deceptive acts or practices in or affecting commerce.” Compare the FTC’s civil enforcement action to the private consumer lawsuit in *DoubleClick*. Does the FTC have any advantages? Disadvantages?
2. Was there anything wrong with Snapchat’s features, or just with how they were described?

3. No statute or regulation specifically tells companies that “reasonable” security measures include “two-factor-authentication” techniques like sending SMS messages to confirm a user’s phone number. But the FTC dinged Snapchat anyway for failing to use two-factor-authentication. Did Snapchat have reasonable notice of its legal obligations? What about future companies deciding what security measures to employ in light of Snapchat?

4. People send each other all kinds of things on Snapchat, and post all kinds of things on Facebook and other social media services. Does this mean that people no longer care about privacy, and the FTC should get out of the way?

5. The consent decree’s remedies are all forward-looking: they are attempts to reform Snapchat’s privacy practices in the future, rather than to penalize it for its past conduct. How effective will they be? If Snapchat already has a duty not to commit “unfair or deceptive acts,” is the consent decree redundant?

6. One recent survey found that six out of ten Americans surveyed responded “true” to the question, “If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.” Are they correct? After reading In re Snapchat, are you inclined to change your online behavior?

7. California has a “data breach law” requiring companies to inform consumers whose personal information (such as social security number, driver’s license number, or credit card number) is acquired by unauthorized persons. What is the purpose of this kind of notification law? How effective do you think it will be in limiting security breaches?

**COOKIE MONSTER PROBLEM**

Cookie Monster is a browser extension that eats cookies. Users install it by downloading it from the Cookie Monster website. After that, every fifteen minutes, it deletes all third-party cookies of the sort used by DoubleClick and other advertising networks. Consumers can turn off Cookie Monster for a particular website by clicking a button in the top left corner of the browser window.

Ozalytics is a “website analytics” service used by websites to keep track of how many visitors they have and what those visitors are doing on the site. It works very much like advertising networks (and Twitter “tweet this” buttons, for that matter): by embedding a small image hosted at ozalytics.com into every page on a website that uses its service. That image can then set a cookie in the user’s browser to track the user’s engagement with the website.

Unfortunately for Ozalytics, Cookie Monster deletes its cookies, making the information it returns to websites much less useful. Ozalytics has responded by asking host websites to include a “Cookie Monster workaround,” consisting of little bit of Ozalytics JavaScript code on each webpage, in addition to the Ozalytics image. That code instructs the user’s browser to simulate a mouse click on the corner of the window where the button to disable Cookie Monster for that website is located.

You represent SometimeSnack.com, a website devoted to healthy cooking tips for parents. You have been asked to consider whether to implement Ozalytics’ proposed Cookie Monster workaround, and if so, how to do it. What is your advice?
F. An International Perspective

In the European Union (E.U.), privacy is considered a fundamental right; privacy laws are both stronger and more general than in the United States. Article 8 of the Charter of Fundamental Rights of the European Union gives all people “the right to the protection of personal data concerning him or her.” The Data Protection Directive of 1995 (DPD) implements these rights in more detail by requiring each country in the EU to have strong privacy legislation. This section sets out the key passages from the DPD, along with some recent decisions from the European Court of Justice (CJEU) – a loose European parallel to the United States Supreme Court – that show some of the recent controversies raised by the DPD and Europe’s increasingly strong commitments to privacy. Note that DPD will be updated with a new General Data Protection Regulation which will take effect in May 2018.

**DATA PROTECTION DIRECTIVE**

*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

*1995 O.J. (L 281) 31*

**Art. 1 – Object of the Directive**

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. ...  

**Art. 2 – Definitions**

For the purposes of this Directive:

(a) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; ...

(d) ‘controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; ...

**Art. 6**

1. Member States shall provide that personal data must be:

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further
processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed....

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Art. 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject ...

Art. 12 – Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; ... 

**Art. 13 – Exemptions and restrictions**

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
   
   (a) national security;
   (b) defence;
   (c) public security;
   (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
   (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
   (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
   (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

**Art. 14 – The data subject’s right to object**

Member States shall grant the data subject the right:

   (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him ... . Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

   (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing ...

**Art. 15 – Automated individual decisions**

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. ...

**Art. 17 – Security of processing**

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unautho-
rized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. ... 

Art. 25 – Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. ...

Art. 28 – Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. ...

QUESTIONS

1. How does the European approach to the privacy of personal data compare with the American approach discussed above?

2. United States privacy law is usually referred to as “sectoral” because it applies to specific types of information. For example, the Children’s Online Privacy Protection Act (COPPA) prohibits collecting private information from children under 13 without parental consent, and the Video Privacy Protection Act prohibits the disclosure of any “personally identifiable information” about consumers who rent or buy “prerecorded video cassette tapes or similar audio visual materials.” The most rigorous such law is probably the Health Insurance Portability and Accountability Act, which imposes quite rigorous confidentiality and security obligations on medical professionals and those working with health records. Should the United States switch to the European approach, or are tailored privacy protections better?

3. What do you make of Article 15’s prohibition on decision-making “solely on automated processing of [personal] data?” Credit checks are ubiquitous in the United States, not just when applying for loans but also in applying for jobs and leases. How would they fare under the Data Protection Directive?

EUROPEAN UNION: ECJ INVALIDATES DATA RETENTION DIRECTIVE

On April 8, 2014, the Grand Chamber of the Court of Justice of the European Union (ECJ) delivered a much-anticipated judgment concerning the legality of
Directive No. 2006/24/EC, commonly referred to as the Data Retention Directive. The Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union.

The Data Retention Directive required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or register user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialed, and call forwarding or call transfer records. The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism. The content of the communications of individuals was not retained.

In considering the broad category of data to be retained, the ECJ observed that such data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environment.

The Court observed that under such circumstances, even though it is not permissible to retain the content of communications, it is possible that the freedom of expression of subscribers or registered users might be in jeopardy.

The ECJ stated that the retention of data in order to allow access by the competent national authorities constitutes processing of data and therefore affects two basic rights of the Charter of Fundamental Rights: (a) the right to private life guaranteed by article 7, and (b) the protection of personal data guaranteed by article 8. ...

Article 52(1) of the Charter requires that any limitation on the exercise of rights guaranteed by the Charter must be provided by law and must respect the essence of such rights. Any limitations are subject to a proportionality test and can be imposed only if they are necessary and meet the objectives of general interest as recognized by the EU or the need to protect the rights and freedoms of others. ...

The Court reasoned that ... the Directive does not establish clear and precise rules that regulate the “extent of interference with the fundamental rights of Art. 7 and 8 of the Charter.” Therefore, it concluded that the Directive “entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what it is strictly necessary.” ...

The Data Retention Directive becomes invalid ab initio, that is from the time it became effective in 2006, since the ECJ did not specify otherwise. The EU Members that have transposed the Directive into their national legal systems are required to take steps to ensure compliance with the judgment.
14. On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the [Agencia Española de Protección de Datos (Spanish Data Protection Agency) (AEPD)] a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) (‘La Vanguardia’), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González’s name in the search engine of the Google group (‘Google Search’), he would obtain links to two pages of La Vanguardia’s newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González’s name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

15. By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

16. By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

17. On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

18. Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). ...
19. That court states in the order for reference that the actions raise the question of what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties’ websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive's publication.

20. In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling …

**Consideration of the questions referred**

**Question 2(a) and (b), concerning the material scope of Directive 95/46**

21. By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the ‘controller’ in respect of that processing of the personal data, within the meaning of that provision.

22. According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties’ web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as ‘data processing’, the operator of a search engine cannot be regarded as a ‘controller’ in respect of that processing since it has no knowledge of those data and does not exercise control over the data. …

25. Article 2(b) of Directive 95/46 defines ‘processing of personal data’ as ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’. …

27. So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus ‘personal data’ within the meaning of Article 2(a) of that directive.
Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine ‘collects’ such data which it subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and, as the case may be, ‘discloses’ and ‘makes available’ to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as ‘processing’ within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

[The court then found that Google was the “controller” of the processing of personal data by its search engine because “the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out.”]

**Question 1(a) to (d), concerning the territorial scope of Directive 95/46** …

**Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46**

By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

Google Spain and Google Inc. submit that, by virtue of the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. Furthermore, to require the operator of a search engine to withdraw information published on the internet from its indexes would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of that operator itself.
66. First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data. ...

72. Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed ‘fairly and lawfully’, that they are ‘collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes’, that they are ‘adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed’, that they are ‘accurate and, where necessary, kept up to date’ and, finally, that they are ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed’. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified. ...

74. This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject – in particular his right to privacy with respect to the processing of personal data ...

76. Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right … to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. ...

77. Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

78. In this connection … each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and … has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.

79. It is in the light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject’s rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.

80. It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that
at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual’s name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous.

81. In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject’s fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject’s rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

82. ... when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages published by third parties containing information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information – from the web page on which they were published. ...

84. Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites. ...

87. Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person’s name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the
Chapter 4: Privacy

313

data subject’s fundamental right to privacy than the publication on the web page.

88. In the light of all the foregoing considerations ... the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages ... even, as the case may be, when its publication in itself on those pages is lawful.

Question 3, concerning the scope of the data subject’s rights guaranteed by Directive 95/46

89. By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove [links] on the ground that that information may be prejudicial to him or that he wishes it to be ‘forgotten’ after a certain time. ...

93. ... even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94. Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased. ...

97. [The rights of the data subject] override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

98. As regards [Mr. González], it should be held that, having regard to the sensitivity for the data subject’s private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, ... require those links to be removed from the list of results. ...
QUESTIONS
1. Some observers have referred to this decision as creating a “right to be forgotten” in the EU. Does it?
2. After Google Spain, what process does someone in the EU need to follow to have unflattering search results removed from search engines? Who will make the ultimate decision on whether the results will be removed, and what evidence will they consider?
3. What result under United States law? Why?
4. What does Google need to do to comply with this and similar requests? What do you find when you search for [Costeja González] on google.com and on google.es?

SCHREMS V. DATA PROTECTION COMMISSIONER
European Court of Justice
ECLI:EU:C:2015:650


2. The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner (‘the Commissioner’) concerning the latter’s refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd (‘Facebook Ireland’) transfers the personal data of its users to the United States of America and keeps it on servers located in that country. ...

LEGAL CONTEXT ...
Decision 2000/520 ...

[The preamble to Decision 2000/520 states:

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States ... issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs. ...

Article 1 of Decision 2000/520 states:

2. In relation to each transfer of data the following conditions shall be met:
(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles ...

The safe harbor principles state:

**NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

**CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

**ONWARD TRANSFER:** To disclose information to a third party, organizations must apply the Notice and Choice Principles ...

**SECURITY:** Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

**DATA INTEGRITY:** Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual’s complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

[The court reviewed two communications adopted by the European Commission on November 27, 2013 based on reports from an ad hoc EU-US working group. Rebuilding Trust in EU-US Data Flows (COM(2013) 846 final) stated in part that ‘[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]’ and that ‘[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme.’ The Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final) observed that 246 companies were self-certified under the safe harbor but, “in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.” Moreover, “safeguards that are provided under US law are mostly available to US citizens or legal residents” and “there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes.”]

**The dispute in the main proceedings and the questions referred for a preliminary ruling**

26. Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network (‘Facebook’) since 2008.

27. Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland’s users who reside in the European Union is transferred to servers belonging to
Facebook Inc. that are located in the United States, where it undergoes processing.

28. On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency (‘the NSA').

29. Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.

30. Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

31. According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale. ...

35. The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

36. In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:
(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administrating and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?

**Consideration of the questions referred...**

The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive...

Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

**The validity of Decision 2000/520...**

As is apparent from the referring court’s explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. ... Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances ... it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter. ...

**Article 1 of Decision 2000/520...**

 Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection ‘by reason of its domestic law or ... international commitments’, the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and
the right to protection of personal data, to be identified and punished in practice.

82. In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are ‘intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates’. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them. ...

84. In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, ‘to the extent necessary to meet national security, public interest, or law enforcement requirements’ and ‘by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.’

85. In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles’ applicability is subject, that, ‘[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law’.

86. Thus, Decision 2000/520 lays down that ‘national security, public interest, or law enforcement requirements’ have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them. ...

88. In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89. Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. ... [P]rocedures before the Federal Trade Commission — the powers of which ... are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

90. Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission’s own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final ... the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly
necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased. ...

92. Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary.

93. Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.

94. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.

95. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. ...

96. In order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

97. However, the Commission did not state, in Decision 2000/520, that the United States in fact ‘ensures’ an adequate level of protection by reason of its domestic law or its international commitments.

98. Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid. ...

**QUESTIONS**

1. What is wrong with the safe harbor framework? Could it be fixed if the European Commission made the appropriate statements in reenacting the safe harbor? Could it be fixed with more detailed voluntary commitments by U.S. companies? With realistically feasible changes to U.S. law? Or is the divide between U.S. and E.U. approaches to privacy so fundamental that no cross-border data transfers will be feasible going forward?

2. One of the most notable revelations in the Snowden leaks was the extent to which the NSA collaborated with foreign intelligence agencies on mass
surveillance projects. Is it hypocritical of the CJEU to invalidate the safe harbor on the basis of privacy violations of the sort European intelligence agencies are themselves deeply implicated in?

3. Does the rule against transfers of data to non-E.U. countries depend on an outdated concept of data having a physical location?