INTEREST CONVERGENCE AND THE ROLE OF CITIZENS AS DEFENDERS OF PRIVACY

by **Steve FRIEDLAND**, Professor of law and senior scholar, the Elon University.

In February of 2016, the United States Government asked a federal court to order Apple, Inc. to create software that would enable the government to bypass a security feature on the cell phone of one of Syed Farook, one of the killers who went on a shooting rampage in San Bernardino, California, in December of 2015.[1]

Apple versus the United States government, including agencies, such as the FBI, the NSA, and the Attorney General, offers unlikely adversaries. Until Apple, Inc., began encrypting the software in its cell phones, government access to phone transmissions was relatively easy to obtain. But the adoption of "technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy the Fourth Amendment's warrant requirements,"[2] created this stand-off, and the Government's particular fear of "going dark," where the Government would have no information about communications,[3] has exacerbated it.

Perhaps more importantly, until several years ago, there were few incentives by private companies to stand on the side of privacy protection. Companies routinely acquired and aggregated user information.[4] Companies like Google, Axiom, AT&T, Verizon, Facebook and others would come by user information naturally. That information was valuable.

Until recently, there was no incentive to protect or maximize privacy. Now, private companies have an incentive to protect privacy. Whether the incentive is pecuniary, with privacy now a brand, or moral or political, many of the larger companies are aligning with Apple in its fight against the government.

This paper suggests the alignment may be explained in large part to interest convergence. The late Professor Derrick Bell advanced this theory as an explanation for societal change in segregation after WWII, helping to explain *Brown v. Board of Education* as a shift favoring the majority Whites as well as the minority African-Americans.

This paper further argues that interest convergence can be utilized to promote privacy for the average citizen, while still allowing the

[1] Eric Lichtblau, and Katie Benner, *As Apple Resists, Encryption Fray Erupts in Battle*, A1 N.Y. TIMES (Feb. 18, 2016).
[2] *Don't Panic*, The Berkman Center for Internet & Society at Harvard University (Feb. 1, 2016).
[3] *Id.*
[4] *Id.*

government to fight crime effectively. The means creating settled expectations about how companies will assist governments in crime interdiction, labeling – like food ingredients – what companies do with the information they receive and how they approach personal privacy. Interest convergence will lead to gradations and distinctive types of privacy. Gradations can include limited disclosures of information, and archetypes can include informational, locational and structural privacy. Above all, because the advancing technologies will keep advancing, the government will have to work with companies or by itself to adapt or new technological architectures. Citizens will rely more and more on education and favorable alignments with companies. Reliance on the Fourth Amendment, unless the 'third-party rule' is significantly adapted to the 21st century, will continue to offer little support.

§ 1 – Why Apple, Inc., is Resisting the United States Government's Request

A) History: Complicit Phone and Tech Companies

In the earlier days of the digital era, in the late 20th Century and early 21st Century, there were numerous partnerships between the government and private technology and telephony companies.
Governments were long able to access information directly from individuals or with the knowing or unknowing assistance of private entities. The government-technology company "partnership" stretches back decades to the Cold War in the mid-20th century, as well as from the war on terrorism.[5] Instead of just using individuals to act as confidential informants as it mostly did for centuries, the government also has been increasingly using private technology and phone companies, such as AT&T, to obtain, aggregate and apply terabytes of information. These companies have in effect become a new wave of informants.
Another government strategy had been to encourage companies, such as Google and Apple, to leave "back doors" or "keys" to encrypted software for government use.[6] Through this strategy, the government was able to "stockpile flaws in software – known as zero days – for future use against adversaries."[7] This stockpiling

[5] *See* David Sanger & Nicole Perlroth, *Obama Heads to Security Talks Amid Tensions*, N.Y. TIMES (Feb. 13, 2014), http://www.nytimes.com/ 2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html (last visited June 16, 2015) (noting a "long history of quiet cooperation between Washington and America's top technology companies") (on file with the Washington and Lee Law Review); Trevor Timm, *Building Backdoors Into Encryption Isn't Only Bad For China, Mr. President*, THE GUARDIAN (Mar. 4, 2015, 11:15 AM), http://www.theguardian.com/commentisfree/2015/mar/04/backdoors-encryption-china-apple-google-nsa (last visited June 16, 2015) (criticizing the U.S. government because the NSA and FBI are pushing for a law that requires technology companies to create encryption keys for the U.S. government while condemning China's plan to require technology companies to do the same) (on file with the Washington and Lee Law Review).

[6] *See* Sanger & Perlroth, *supra* note 5 (discussing top technology companies' resistance to U.S. government efforts to force technology companies to install back doors or encryption keys in their products so the U.S. government can gain access).

[7] *Id.*

also apparently allowed the NSA to tap into traffic between Google's servers because of a security flaw.[8]
An additional method the government has at its disposal to obtain information is the silent subpoena. It is silent because the subject does not know about its use because of secrecy concerns. The subpoena is all that is needed to accumulate mountains of data.[9]

B) The Stakes

On December 2, 2015, Syed Farook and his wife, Tashfeen Malik, attacked co-workers at a holiday gathering, killing 14. In a shoot-out with the police, they were both killed. The federal government investigated the case, especially to determine whether the Islamic State, known as ISIS, was involved in any way.
The government's investigation apparently stopped at Mr. Farook's locked iPhone. While the government apparently tried to open the phone and succeeded in changing the password, the police were unsuccessful. With Apple's strong encryption, it apparently could not open the phone;[10] nor would Apple agree to help it do so. According to Reynaldo Tariche, a FBI agent and president of the agents' association, "the worst-case scenario has come true. As more of these devices come to market, this touches all aspects of the cases that we're working on."[11]
A federal magistrate judge ordered Apple on February 16, 2016, to assist the FBI in unlocking an iPhone used by Farook. The government had claimed that the phone could have "crucial evidence" on it about the San Bernardino attack.[12] The 5 C version iPhone in question was put out to market in 2013 and has a passcode that locks it through encrypted software.[13] The court required Apple to help the government "bypass or disable" the feature of the phone that will automatically wipe the phone clean of all of its data if 10 incorrect passwords are entered in a row. If this feature is disabled, the government could use "brute force" methods to obtain the phone's passcode, hooking it up to a computer to enter millions of passcodes to guess the correct one. Apple claims that if it builds new iOS software to bypass the restriction, it potentially can be applied to all iPhones, not just the

[8] *See id.* (noting reports of the NSA's interception of email traffic moving between Google and Yahoo servers). But the relationship appears to be troubled. According to the cybersecurity coordinator for the Obama Administration, Michael Daniel stated, "American firms are increasingly concerned about international competitiveness, and that means making a very public show of their efforts to defeat American intelligence gathering by installing newer, harder-to-break encryption systems and demonstrating their distance from the United States government." *Id.*
[9] Companies are trying to circumvent these subpoenas by creating encrypted technology "that the firms themselves cannot break into—meaning they cannot turn over emails or pictures, even if served with a court order." *Id.*
[10] Eric Lichtblau, and Katie Benner, *As Apple Resists, Encryption Fray Erupts in Battle*, A1 N.Y. TIMES (Feb. 18, 2016).
[11] Mike Isaac, *Why Apple Is Putting Up a Fight Over Privacy with the F.B.I.*, N.Y. TIMES B 4 (Feb. 18, 2016).
[12] Mike Levine, Jack Date, and Jack Cloherty, *DOJ Escalates Battle with Apple Over San Bernardion Shooter's Phone*, ABC NEWS (Feb. 19, 2016) www.abcnew.go.com/US/doh-escalates-battle-apple-san-bernardino.
[13] *Id.*

one in question.[14] While Apple can create the new software, it claims such software does not currently exist. The CEO of Apple, Tim Cook, wrote in his letter opposing the government's request, "The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe."[15]

There might be alternative methods for the FBI to obtain the information it seeks. It could seek additional information from Verizon, the cell phone carrier used by Farook, or try to obtain information from the developers of the applications on the iPhone in question.

Apple recently won a similar case on February 29, 2016, in the Eastern District of New York.[16] There, the government claimed that Apple's assistance would help with a search warrant and was justified under the All Writs Act, 28 U.S.C. Section 1651, as was the justification in the San Bernardino case. The AWA was used as a residual authority for the magistrate to issue such an order of compliance. The magistrate judge, in a 50-page memorandum order, decided not to force Apple to create an easier route toward discovering phone contents. The Judge held:

> "For the reasons set forth below, I conclude that under the circumstances of this case, the government has failed to establish either that the AWA permits the relief it seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion. More specifically, the established rules for interpreting a statute's text constrain me to reject the government's interpretation that the AWA empowers a court to grant any relief not outright prohibited by law. Under a more appropriate understanding of the AWA's function as a source of residual authority to issue orders that are "agreeable to the usages and principles of law," 28 U.S.C. § 1651(a), the relief the government seeks is unavailable because Congress has considered legislation that would achieve the same result but has not adopted it. In addition, applicable case law requires me to consider three factors in deciding whether to issue an order under the AWA: the closeness of Apple's relationship to the underlying criminal conduct and government investigation; the burden the requested order would impose on Apple; and the necessity of imposing such a burden on Apple. As explained below, after reviewing the facts in the record and the parties' arguments, I conclude that none of those factors justifies imposing on Apple the obligation to assist the government's investigation against its will. I therefore deny the motion."[17]

[14] *Id.*
[15] *Id.*
[16] *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By This Court*, Case 1:15mc-01902-JO (Judge Orenstien) (Feb. 29, 2016).
[17] *Id.*

Thus, the essential issue in these cases is whether forced assistance will become precedent for other government requests of Apple, or requests of other tech companies, by the American or foreign governments. In the alternative, should the structure for government-private technology company cooperation will be set by the legislature.
In fact, the dispute is now partially shifting to the halls of the legislature. The House of Representatives Committee on the Judiciary has called a hearing, "The Encryption Tightrope: Balancing Americans' Security and Privacy."[18]

§ 2 – WHY PRIVACY HAS BEEN DIMINISHING

> "It won't be a question anymore of whether things are connected. We're going to move toward a learning model where your home actually observes how you're living inside it and adapts itself toward your needs."
> George Yianni[19]

A) A Shifting Field of Engagement – What is a Phone Booth?

When the seminal American case defining the contours of privacy under the Fourth Amendment, *Katz v. United States*,[20] involves an item many people born-digital have never seen – a phone booth, it is not surprising that the protections afforded under the Amendment don't seem to adapt well to advancing technologies.

1) Structural and Cultural Advances

The world has changed since *Katz* was decided in fundamental socio-cultural, economic, political and technological, ways. As the digital era emerged, and regularly used devices tracked and aggregated trillions of bytes of data, it became commonplace to aggregate and sort the data points. These data points were very valuable, providing information on habits of consumers, and the propensities of voters, workers, and even criminals. This data was commoditized and support markets occupied by data creators and data brokers.
Mechanisms accumulating data range from Global Positioning Systems, to drones, to encryption-piercing tools, to Internet cookies, to the Internet of Things.[21] A smart device like a

[18] *See*, U.S. House of Representatives Judiciary Committee, *Hearings*. http://judiciary.house.gov/index.cfm/hearings?ID=89431275-E911-4D5C-BD70-BFE3EF91AD86 .
[19] Yianni invented the Philips Hue connected light bulb.
[20] 389 U.S. 347 (1967).
[21] The Internet of Things refers to devices that generate data and can be operated and adjusted remotely. See, e.g., Kyle Vanhemert, *This Brilliant Washing Machine is a Roadmap for the Internet of Things*, WIRED, (April 7, 2014, 6:30 AM):

thermostat creates better-regulated temperatures, but also generates reams of data for the companies that make the device and other third parties.

The new Internet of Things, where common things have connective and information-generating properties, splits form and function. The "smart" thermostat, for example, generates bulk data that tracks how and when the home is being used.[22]

The smart watch takes Dick Tracy's cartoon world and makes it a functional reality. A Pebble watch, just one of many smart watches offered for sale, is customizable, contains Internet-connected applications, and is capable of connecting to iPhone and Android phones via Bluetooth.[23] The watch tells time, but has other functions: it computes, has apps, and even the capability of making phone calls. While it might be worn as a watch, it is less a watch than simply another form of interconnective device. Smart glasses have been developed as well. For example, Google created Google Glass—a device worn like a pair of eyeglasses, but a name that is more of a misnomer than accurate, given it is a multifunctional device, not a monolithic tool. While not being actively marketed, Google Glass can record what the wearer sees, can send a message by telling it to do so, and can share what is seen.

The data generated by "smart" home devices and wearable technology travels invisibly and often a long way, sometimes with numerous stops from one company to the next. This data traveling has considerable legal significance.[24] While the homeowner initially controls all of the devices, the information can be accumulated and transferred to the commercial marketplace by the device creator. That information, ultimately, can end up with the government.[25]

The nature, quantity, and quality of information produced by devices whose form and function are separated will be extensive. These devices are smart because they "learn" to become more efficient – the lighting device can "learn" the "household's daily patterns over time and set itself to turn on the lights just before the family starts arriving home in the evening." The lighting mechanism can even learn to turn on low light when the occupant gets out of bed at night. The television can be triggered by voice activation, which means it can listen" to the speaker and anyone else talking in the room in which the set is located.[26] The smart

---

http://www.wired.com/2014/04/this-brilliant-internet-connected-washer-is-a-roadmap-for-the-internet-of-things/. (describing Cloudwash, a prototype washing machine by Berg Co.).

[22] *See*, e.g., the Next Thermostat, that determines whether someone is home and automatically adjusts the temperature in the home. The company was recently purchased by Google for 3.2 billion dollars. Josh Ong, *Google to Acquire Nest Labs for $3.2 Billion*, TNW BLOG, Jan. 13, 2014, http://thenextweb.com/google/2014/01/13/google-acquires-nest-3-2-billion/.

[23] Pebble: E-Paper Watch for iPhone and Android, KICKSTARTER, https://www.kickstarter.com/projects/597507018/pebble-e-paper-watch-for-iphone-and-android, <http://perma.cc/LCC9-4E6F>.

[24] *See* Part II.B (contending that the amount of data collected by smart technology creates unprecedented opportunities for surveillance).

[25] *See* Part II.A.2 (discussing the government's use of private companies to gather data about Americans).

[26] *See, e.g.*, *Not In Front of the Telly: Warning Over 'Listening' TV*, BBC (Feb. 9, 2015, 6:20

thermostat can reveal whether anyone is in the house, how long occupants slept the night before, and which rooms are likely occupied, automatically lowering the thermostat in unoccupied areas to save energy.[27] The thermostat "learns" about the inhabitants and their propensities at home.[28] The watch provides the time, but can monitor the wearer – determining how many steps the person is taking in a day to show levels of activity, how well the wearer slept the night before, and even how the heart, a vital organ, is beating.[29]

The car has changed as well. It now can be started remotely, which provides more time indoors for the driver, but also adds to the accumulated data points about the car's driving history[30] – from "where drivers have been, like physical location recorded at regular intervals, [to] the last location they were parked, distances and times traveled, and previous destinations entered into navigation systems."[31] Soon, vehicle-to-vehicle communication will occur, with cars sharing information.[32] This will become an even larger data source when driverless cars emerge in the not so distant future.

Such structural advances in technology seem to emerge almost daily. One of the largest billboard companies in the United States recently announced that it would use its billboards to track the cell phones and devices of passersby through a software program called Radar:

> "Using anonymous aggregated data from consumer cellular and mobile devices, RADAR measures consumer's real-world travel patterns and behaviors as they move through their day, analyzing data on direction of travel, billboard viewability, and visits to specific destinations. This movement is then mapped against Clear Channel's displays,

---

PM), http://www.bbc.com/news/technology-31296188 (last visited June 16, 2015) (on file with the Washington and Lee Law Review) As stated in the article: The policy explains that the TV set will be listening to people in the same room to try to spot when commands or queries are issued via the remote. *Id.* It goes on to say: "If your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party." *Id.*

[27] *See* Kashmir Hill, *When Smart Homes Get Hacked: I Haunted a Complete Stranger's House Via the Internet*, FORBES, (July 26, 2013, 9:15 AM) http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/ (last visited June 16, 2015) (describing a thermostat that monitors inhabitants' activity, learns their schedules and temperature preferences, and heats or cools the house as it deems appropriate) (on file with the Washington and Lee Law Review).

[28] *Nest Thermostat*, NEST, https://nest.com/ie/thermostat/meet-nest-thermostat/ (last visited June 16, 2015) (describing the features of a smart thermostat) (on file with the Washington and Lee Law Review).

[29] *See, e.g.*, *Fitbit*, FITBIT http://www.fitbit.com/#i.1r2ovyecs6fal1 (last visited June 16, 2015) (on file with the Washington and Lee Law Review). The Fitbit can be placed on one's belt or around one's wrist. *Id.* In addition to keeping time, it can mark steps, sleep time and restfulness, heartbeats, and more. It can be linked to the Internet to store this information. *Id.*

[30] This information is shared with the manufacture and third parties. Aaron M. Kessler, *Report Sees Weak Security In Cars' Wireless Systems*, N.Y. TIMES, Feb. 9, 2015, at B4, *available at* http://www.nytimes.com/2015/02/09/business/report-sees-weak-security-in-cars-wireless-systems.html?_r=0.

[31] *Id.*

[32] *See id.* (noting vehicle-to-vehicle communication is expected to be available in the near future). While industry trade groups pushed to limit data collected for legitimate business purposes, a report by Senator Edward J. Markey, Democrat of Massachusetts, "says the phrase 'legitimate business purposes' is vague enough to allow for all kinds of collection, and asserts that clear federal rules should be established for what are permissible and appropriate uses of drivers' data." *Id.*

> allowing advertisers to plan and buy Out-Of-Home to reach specific behavioral audience segments."[33]

The company is starting its marketing in major cities and then spreading nationwide by the end of the year.[34] Clear Channel Outdoors argued that this form of marketing differs from the personalized marketing endured by Tom Cruise's character, John Anderton, in the futuristic thriller, M*inority Report,* because the Clear Channel company can only aggregate the data, not personalize it as in the film.[35] Yet, the company's methodology has been called "creepy"[36] because people are completely unaware of the tracking that is occurring.

2) Advanced Hacking

A corollary to the advances in technology has been the advances in hacking the software and databases of another. Cyber breaches have become the new battleground for many skirmishes, often unseen except by participants. The cyber breaches have been occurring with greater frequency and magnitudes, both public and private. In 2014, SONY experienced a very pubic hack in which its computer system was compromised.[37] The hack led to the disclosure of emails by executives and others designed to dissuade it from releasing a movie about North Korea's dictator, The Interview – which it initially did not release as a result of the threats.[38] The U.S. government Office of Personnel Management had the personal information of more than 21 million former and current employees hacked,[39] and in the past two years alone had cyber breaches in the server supporting the Department of Health and Human Services, the National Oceanic and Atmospheric Agency, the United States Postal Service, the Department of State, the Federal Aviation Administration, the Department of the Defense, and the Internal Revenue Service.[40] Cyber threats come from many different countries and they will continue to occur, likely at an increased pace. While information sharing and partnering with internationally are two defenses against these risks,

---

[33] Merrit Kennedy, *Using Billboards, Company Will Collect Personal Information to Help Advertisers*, THE TWO-WAY, NPR (Feb. 29, 2016). http://www.npr.org/sections/thetwo-way/2016/02/29/468598100/using-billboards-company-will-collect-personal-information-to-help-advertisers.

[34] *Id.*

[35] *Id.*

[36] Jeffrey Chester, Executive Director of the Center for Digital Democracy. *Id.*

[37] BBC News Broadcasting, *The Interview: A Guide to the Cyber Attack on Hollywood*, (December 29, 2014). http://www.bbc.com/news/entertainment-arts-30512032

[38] *Id.* The 2014 hack was described as follows: "On November 22, there were signs that Sony's computer system had been compromised when skulls appeared on employees' screens with a message threatening to expose "secrets" from data obtained in a sophisticated hack." *Id.*

This initially caused crippling computer problems for workers at Sony, who were forced to work with pen and paper. "We even fired up our fax machine," one employee told the LA Times.

[39] Riley Walters, *Continued Federal Cyber Breaches in 2015*, Issue Brief 4488 (Nov. 19, 2015).

[40] *Id.*

even a multifaceted approach must prepare to confront novel strategies and tactics.

B) New Government Surveillance Techniques

The federal government has been initiating its own advanced techniques, many of which arguably navigate around the Fourth Amendment. The government uses GPS geolocation tracking that, after *Jones v. United States*,[41] does not involve a physical trespass. It also uses Stingray and other IMSI catcher devices that secretly imitate cell-phone towers to obtain location information of cell phones.[42] Courts are often not told about the deployment of these IMSI catcher devices.[43] In February of 2016, it was reported that federal marshals secretly tracked 6,000 cell phones throughout the United States.[44] While the agency did acknowledge using these devises, it opposed a Freedom of Information Act request for a copy of its records.[45] Dozens of police departments also secretly used similar tracking devices.[46] The State of Florida alone tracked 1,600 phones through stingrays.[47]

In Tijuana, Mexico, the police have deployed two battery-operated drones over the city on a 24-hour basis, intending to defend against burglaries and break-ins. The "eyes-in-the-sky" offer an efficient and new way to provide comprehensive coverage around a city. On the other hand, the use of surveillance drones also offers a greater understanding that the government is watching you.

C) Outdated Legislation

The pertinent federal laws protecting data privacy are decades old. Even Congress recognizes that email privacy is insufficient, and needs greater protection.[48] Distinguishing between emails that are more than six months old and newer emails might have been useful at one time, but is certainly not today, as people routinely store thousands of emails in ever-growing storage capacities.

D) Everyone is Surveilling Each Other: "I Know What You (and I) Did ___"

One need only look at a person's wrist to determine the level of self-surveillance that is occurring. Many people now use fitness-tracking wearable devices. These devices track sleep patterns, steps

---

41 132 S.Ct. 935 (2012)

42 *Courts Unaware Stingray Devices Are Used*, 1A USA TODAY (Feb. 24, 2016).

43 Id. Nathan Wessler, an ACLU lawyer, commented, "That's a lot of deployments of a very invasive surveillance tool." *Id.*

44 *Id.*

45 Brad Heath, *Feds Secretly Tracked 6,000 Phones*, USA TODAY (Feb. 24, 2016).

46 *Id. Courts Unaware Stingray Devices Are Used*, 1A USA TODAY (Feb. 24, 2016).

47 *Id.*

48 Erin Kelly, *Congress looks to Boost Email Privacy, Increase Scrutiny of Social Media*, USA TODAY (Feb. 22, 2016) ("Congress is moving to protect Americans' emails from government snooping while also urging federal agents to keep closer tabs on social media to check for possible terrorist communication." *Id.*)

taken each day, heart rates, blood sugar, food intake, and even detect mood patterns over time.[49] The information can be synced to mobile phones and other devices.[50] Significantly, while this information is often meant only for the wearer of the device or the wearer and physician, it is stored and shared by up to several different entities[51] – and sometimes makes it way to the government.

E) The Incredible Shrinking Fourth Amendment. The Third-Party Rule

Under the progeny of *Katz v. United States*,[52] namely *United States v. White*, (dealing with "false friends"), *Smith v. Maryland*[53] (and pen registers), and *United States v. Miller*[54] (and bank depositors), the "third party" rule developed. This rule decrees that information knowingly disclosed to third parties is effectively no longer private under the Fourth Amendment, even though limited disclosure might have been subjectively intended. The implications of this rule are huge, and many areas of people's lives, from health, to financial to family, are no longer beyond discovery and transfer to others.

§ 3 – Ways to Promote Privacy In a Shifting Field of Engagement

> "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."
> Thurgood Marshall, dissenting, *Smith v. Maryland*, 442 US 735 (1979)

A) How Interest Convergence Theory Promotes Privacy

> "Turn and face the strange."
> David Bowie

Interest convergence theory suggests that convergent interests can explain how groups that appear to be opposed might in fact align.[55]

---

[49] Kate Crawford, *When Fitbit Is the Expert Witness*, The Atlantic (Nov. 19, 2014).
[50] Jeffrey Norris, *Health App Technology Explored at Medicine X 2012 Symposium*, UCSF Website (Oct. 5 2012).
[51] Kate Crawford, At 2.
[52] 389 U.S. 347 (1967).
[53] 442 U.S. 735 (1979).
[54] 425 U.S. 435 (1976).
[55] *See, e.g.,* Derrick A. Bell Jr., *Brown v. Board of Education and the Interest Convergence Dilemma*, 93 Harv. L. Rev. 518 (1980). *See* also, Sheryll D. Cashin, "Shall We Overcome?

One group can be accommodated by the other, but only if the benefits to the other group justify the alliance.[56] While proposed by Professor Derrick Bell in the context of affirmative action,[57] the theory also applies in the context of digital privacy.

Today, it is clear that the interests of individuals and mammoth technology companies have become more aligned, with the large companies having a pecuniary interest to protect customers' privacy – while at the same time engaging in data collection and brokering. The companies object to forced disclosures by the government and in this regard have become more overtly libertarian in nature – if disclosures are to occur, it is up to the companies themselves to make the decision whether to do so.

Interest convergence creates strange combinations or bedfellows. For example, the former CIA and NSA chief, retired general Michael Hayden, has come out vocally on the side of privacy. Hayden stated, "In this specific case, I'm trending toward the government, but I've got to tell you in general I oppose the government's effort."[58] He added, "I think on balance that [a back door] actually harms American safety and security, even though it might make (the FBI's) job a bit easier in some specific circumstances."[59]

1) Promote Interest Convergence Through Culture and Legislation

Interest convergence is not restricted to Apple and its users; it is apparent in other countries around the world as well. Privacy is both a value and a brand. In a sense, it has turned into both a right and a commodity. On many international websites, the use of cookies, and what they are used for, are prominently displayed. Users are asked to accept the presence of cookies prior to using the site. Some examples follow:

> "This website or third-party tools used by this website use cookie necessary for the operation and useful to the purposes' shown in cookie policy. To continue the navigation, click on 'Accept' button otherwise, you can opt out or see the cookie policy."[60]
>
> "This website does NOT use Cookies for profiling, but only for traffic analysis in order to improve your experience

Transcending Race, Class and Ideology through Interest Convergence," 79 St. Johns L. Rev.253 (2012).

[56] *Id.* This approach was taken by Professor Bell regarding the reason why the Supreme Court changed its position on integration.

[57] *See, e.g.*, Justin Driver, *Rethinking the Interest-Convergence Thesis*, 105 NORTHWESTERN L. REV. 149 (2011) ("The Court's decision in *Brown*, by these lights, was not motivated by a desire to redress black suffering un- der racial segregation; instead, the United States eliminated Jim Crow in order to improve its international image during the Cold War." Id.)

[58] Susan Page, *Ex-CIA Chief: Apple Is Right*, Capital Download, USA TODAY (Feb. 22, 2016).

[59] *Id.*

[60] [ilcolosseo.it]: http://www.il-colosseo.it/en/cookie-policy.php.

on this website. If you continue, you declare to accept the use of Cookies by this website."[61]

PRIVACY
Having carefully read the PRIVACY STATEMENT I agree that my personal data may be transferred to third parties or to Trenord Srl partners, for statistical surveys for marketing* purposes and/or to receive information and/or promotional communications from third parties.[62] Demand Government Transparency on the Parameters – Apply the First and Fourth Amendments as well as Equal Protection

[61] *See*, Florentown.com.it.. The site further describes what it does with the data it collects:
Compliance with the Italian law on privacy
The customer's personal data is stored by FLORENCETOWN by Worlding Solutions in order to provide reservation services and any other services requested by the user and in order to transmit any related information. In case the data is incomplete or incorrect, it will be impossible to access the reservation services or any other services that require the use of personal data. Personal data will be processed in compliance with Legislative Decree No. 196, June 30th 2003 ("Code regulating the protection of personal data").
FLORENCE TOWN by Worlding Solutions informs that personal data supplied and acquired in relation to a reservation as well as data necessary in order to provide the requested services shall be processed for the following purposes: purposes strictly related to and necessary to access the system, the online booking services, as well as the activation of the booking services; purposes related to the transmission of messages concerning the reservation purposes related to the activities of FLORENCE TOWN by Worlding Solutions, including market researches, economic and statistical analyses, as well as the diffusion of advertising material and commercial communications. Users always have the option to refuse the processing and diffusion of their personal data for the latter purpose. The processing of data provided by the users will comply with principles of fairness, lawfulness, and clearness and will be carried out in full compliance with the abovementioned law, thus ensuring maximum confidentiality and protection of the Customer's rights. The processing will also be carried out by means of electronic or automated devices directly by us and/or by third parties
Providing the required data is compulsory due to the fact that, without such data, access to the system and to its online booking services is impossible. Should the user refuse to provide the necessary data, he/she will not be able to use the system and its booking services. Consequently, it will also be impossible for us to manage and transmit the user's booking requests. The data might be transmitted to third parties designated to provide services connected to the user's reservation; in this case, it will be used solely for the purposes mentioned above.
The Customers declares their being aware of their rights as per article 7 of Legislative Decree no.196/2003, which is summarized below. Article 7 of the Code regulating the protection of personal data grants the Customers the possibility to exert specific rights, among which the right: to receive by FLORENCE TOWN by Worlding Solutions the confirmation of the existence or inexistence of their personal data and to view it in a clear and unambiguous form; to be informed about the source of the data and about the procedure and purposes of its processing; to demand the deletion, transformation into anonymous form or the blocking of any data processed in ways that violate the law, as well as to require updates, corrections, and integrations, when needed; to oppose the processing for legitimate reasons and to oppose, at any given time, the processing of personal data for purposes related to the diffusion of advertising material, the direct sale of products or market researches.
In order to exert such rights, Customers can contact the Manager Responsible for Personal Data Processing by writing to Worlding Solutions s.n.c., Via de' Lamberti 1, 50123 Firenze ITALIA, or calling Switchboard + 39 346 1 525 515.

[62] Trenord.it :
https://sso.trenord.it/UI/RegistrationLight?authority=trenord.it&returnUrl=aHR0cDovL3d3dy50cmVub3JkLml0L2l0L3NlcnZpemkvc2V0c2Vzc2lvbmJ5dG9rZW4uYXNweA.

2) Publicize Transparency Where Interests Converge

If interest convergence is to be effective, there must be sustained efforts to support it. One important way of support is to publicize points of convergence. For example, a federal court recently lifted a gag order on an Internet Service Provider, permitting it to reveal the FBI's demands for various information,[63] including records of user Web browsing history, IP addresses online acquisitions and location information. Of the thousands of national security letters issued by the FBI each year, seeking company records of consumer conduct, this one was one of the first lifted. In fact, recipients of NSLs are prohibited from admitting to the requests.

The Electronic Frontier Foundation publicizes how companies are protecting privacy. The non-profit organization uses six criteria to analyze the level of privacy protection: "follows industry-accepted best practices; tells users about government data demands; discloses policies on data retention; discloses government content removal requests; and pro-user public policy: opposes back doors."[64]

3) Use Interest Convergence to Uptade Fourth Amendment Analysis

a. Fit the Third-Party Rule to the Digital Era – Many Shades of Privacy

Several courts have had the opportunity to review the Third-Party Rule in the face of government collection, storage and usage of "public" information through locational tracking, including the Supreme Court. The Supreme Court, in *Grady v. North Carolina*,[65] has already said the North Carolina legislature went too far in imposing permanent for-life tracking of a parolee.[66]

Appellate and state courts have had that opportunity as well. This is particularly apparent with regard to historical cell site location data. While arguably "knowingly exposed" to third parties and unprotected under the pen register case of *Smith v. Maryland* and the bank depositors' case of *United States v. Miller*, some courts are resisting the temptation of furthering a bright line out-of-step in an era where privacy comes in many shapes and hues, from locational, to informational, to physical, to experiential. As a state court judge, in *Ford v. Texas*,[67] noted in dissenting from an opinion permitting accumulated historical cell site location information in evidence without Fourth Amendment limitations:

---

[63] *See*, *e.g.*, epic.org, Locational Privacy, Latest News.

[64] *See*, Electronic Frontier Foundation, *Who Has Your Back? Protecting Your Data from Government Requests*:
https://www.eff.org/who-has-your-back-government-data-requests-2015.

[65] ___U.S. ___ (2014).

[66] *Grady v. North Carolina*, U.S. (2014).

[67] *Ford v. State*, (Tx. Ct. App. 2014).

> "To achieve this result, the majority relies on *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976). These cases predate the advent of the earliest commercially available handheld cell phones."[68]

The Court proceeded to note:

> "The majority's application of the third-party doctrine sweeps intimate details of a person's life outside the scope of the Fourth Amendment's protections because cell phone customers "voluntarily disclose" their location information simply by owning and using their cell phones. The majority thus confronts cell phone customers with a choice between Scylla and Charybdis: either forego the use of technology that has become a pervasive and insistent part of modern, everyday life or forego the protections of the Fourth Amendment. I cannot join such a sweeping and mechanical application of Smith and Miller.
>
> Instead, I agree with the Third and Eleventh Circuits and conclude that "a cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." In re Application of U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3rd Cir.2010); United States v. Davis, 754 F.3d 1205, 1216–17 (11th Cir.2014). I would therefore hold that Ford did not voluntarily surrender his reasonable expectation of privacy in his physical location and movements simply by using his cell phone. Because the State did not secure a warrant before obtaining the historical cell site data from Ford's cell phone provider, Ford's Fourth Amendment rights were violated, and the trial court should have granted his motion to suppress.
>
> Because the Fourth Amendment required suppression of the historical cell site data, the denial of Ford's motion to suppress was constitutional error."[69]

Significantly, the dissent attacked the passive signals sent form the accused's cell phone as incriminating evidence:

> "The records used by the State to pinpoint Ford's location on the night of Edwards's murder were determined from records of passive activity on his phone, i.e. he was not placing a call when his phone connected with the cell tower. Rather, the records relevant to the State's case, the 11:45 p.m. and 1:19 a.m. "pings" off of the Gallery Court tower, were from a missed call and text message, respectively, from Tarver. None of Ford's active cell phone usage on the night in question, e.g., his response text to Tarver at 11:33 p.m. or his checked voicemail at 2:30 a.m., is located in the

[68] *Id.*
[69] *Id.*

vicinity of the Gallery Court tower near Edwards's residence."[70]

4) Create Government Accountability

Two recurring issues concerning the data being accumulated involve government-piggybacking off of information gathered or sorted by private companies and traveling data, that is passed on from one company to another. Both of these issues are significant in creating government accountability. Government piggybacking should become more controlled and transparent. Private company technological architectures should not automatically become a proprietary interest of the government. Further, information that is passed from one group to the next should be regulated.

Accountability will occur not only with general rules, but also with particularity, deliverables by individuals in government. A good illustration of how to seek accountability involves the N.Y. City lawsuit against the police for violating the requirements of *Terry* stop-and-frisk limitations. The settlement of a lawsuit filed against the city for being overaggressive in their stops and frisks, often of members of minority populations, included requirements that officers create paperwork documenting the suspicion prompting a stop for questioning and a "receipt" to individuals who were stopped and questioned.[71] A follow-up inquiry as to whether police officers were complying with these requirements showed that more than one-quarter of the documents did not have the requisite suspicion for the stop filled out, and that many individuals were not given "receipts" confirming the stop and questioning.[72] An objective of the obligations appears to be changing the police culture as well as specific practices.[73]

CONCLUSIONS

In the digital world, there appeared to be few if any incentives for the government or large technology or telephony companies to protect individual privacy. Private companies, the government and individuals seem to have entirely different interests – companies are interested in their profits and business; government is interested in surveillance and worried about "going dark," and individuals have a plethora of worries, ranging from obtaining Web services, to being hacked, to being shut off the grid. Unless individuals comply with company and government strictures, they are at risk of losing access to Web sites, apps and services.

While many have suggested that the American Constitution should be the primary defender of government overreaching and abuses,

[70] *Id.* At N 2

[71] Al Baker, *City Police Still Struggle to Follow Stop-and-Frisk Rules, Report Says*, A 16 NEW YORK SECTION N.Y. TIMES (Feb. 17, 2016).

[72] *Id., The findings, and others, come from departmental audits.*

[73] "While a police culture cannot transform overnight, mistakes by officers, and their mistreatment of civilians in such encounters, fuels the public's mistrust of law enforcement." *Id.*

it has not played that role, as exemplified by the Fourth Amendment's pre-digital 3rd Party Rule, where information knowingly exposed to a third party loses much if not all of its privacy protection. Instead, a better course of action at the current time appears to be interest convergence theory. This theory focuses on the points of alignment between private companies and individuals. Today, it is clear that privacy is both a value and a brand or, stated another way, privacy shares space as a commodity and a basic personal right. This convergence can lead to increased protection through the publicizing of privacy measures taken by companies – the equivalent of labeling of food ingredients – opposition to secret public-private partnerships with the transfer of information at their heart, and greater transparency about how to promote individual privacy.