DOCKET MEDIA LLC
PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM

CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

MARCH 1, 2016

STARK ON IR

APPLE VERSUS THE FBI: SOME COMMON SENSE REFLECTIONS FROM 'COOL HAND LUKE'

During the 1967 film, "Cool Hand Luke," when tedium in a prison chain gang seems to overtake the inmates, the incarcerated Luke, played by Paul Newman, quietly (and heroically) pronounces to his fellow inmates, "I can eat 50 eggs. "

Amid the excitement surrounding Luke's provocative claim, a gambling frenzy arises and the wager is on. Terms are negotiated among the various believers and non-believers; a rules committee is formed; and Luke agrees to a one-hour time limit in which to eat all 50 eggs.

Dragline, another prisoner, played by George Kennedy (who died just yesterday at age 91), becomes the head of the syndicate backing Luke's claim while the guards, equally engaged, direct the prison cook to prepare 50 hard-boiled eggs for the contest. The countdown for the challenge begins and Dragline immediately begins peeling the eggs and arranging them in front of Luke. A prisoner jailed for counterfeiting nicknamed "Society," who is leading the group betting against Luke, angrily accuses Dragline of cheating, "He peels his own eggs – that is understood!" yells the outraged "Society." Dragline responds, anointing himself as Luke's "official egg peeler," and tells "Society," in one of the best lines of the film:

> "You just may be great at hanging paper around big cities. But country boys like me are not entirely brainless. When it comes to the law, nothing is understood."

Apple CEO Tim Cooke and FBI Director Jim Comey might want to spend a few quality hours watching Cool Hand Luke, perhaps the greatest flick of all time. Because what their dispute boils down to (pun intended) is an area of the law and of societal thinking that is definitely misunderstood.

So much has now been written, argued and pontificated concerning the headline grabbing battle between Apple and the FBI, and what has emerged is a chaotic, bewildering and blurring morass. Not that the battle isn't worthy of all of the attention and hype; it is. The case has brought to light critical and nuanced issues and facts which absolutely necessitate scrutiny and reflection.

However, what's missing from the discussion is some good old-fashioned common sense, which today's *Stark on IR* posting now introduces into this 21st Century technological and legal firestorm.

SOME BACKGROUND

The Device at Issue. The device at issue is an iPhone 5c, used by Syed Rizwan Farook, who with his wife, Tashfeen Malik, opened fire during a holiday party at the Inland Regional Center in the San Bernardino massacre, killing 14 people and injuring 22 others.

The FBI claims that there may be "relevant, critical communications and data" on the iPhone from around the time of the shooting (the FBI has already sought and received from Apple all data from any cloud storage connected to the device).

Apple claims that it cannot unlock its newer iPhones for law enforcement (such as the iPhone 5c), even when presented with a warrant, because its phones are now engineered in such a way that Apple does not hold the decryption key. Specifically, Apple's iOS operating system is designed to automatically erase local data after too many incorrect passcode attempts and only someone knowing the password would be able to unlock the phone.

Though encrypted communication platforms have been available since the early 1990s, the encryption debate began to involve Apple when, in 2014 Apple released its new iOS, which contained a feature that generates random security "keys" that are unknown to Apple and in combination with the user's passcode to decrypt the device's data. Without such mathematical formulas, the personal data is unreadable. This two-step "full disk" encryption process makes iPhones more secure, but it also means Apple cannot unlock its own products. Neither can Google after adopting the same practice.

Because iPhone 5c's (and all later models) can only run software with Apple's proprietary cryptographic signature, the FBI wants Apple to create and upload a custom version of iOS to Farook's device that overrides this mechanism. The FBI would then hook up an external computer that will make unlimited guesses to unlock the phone's contents, known as "brute forcing." That way, for instance, the government can try to crack the password, attempting tens of millions of combinations without risking the deletion of the data.

The Government's Ex Parte Request. Frustrated by Apple's refusal to create the new iOS, the government sought and obtained a court order from U.S. Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California. The government sought the order *ex parte*, which means Apple did not have any opportunity to present any form of opposition to the judge.

It is not clear why the government moved *ex parte* and why the judge granted an order without hearing from Apple. This was not a case where the government needed to proceed in secret to safeguard its investigation; the government did not proceed "under seal," which secretes the motion from public view; and the government presented no extraordinary circumstances as to why Apple should not get the opportunity to oppose the government on the matter. Perhaps the government knew a battle was looming, and by blindsiding Apple with an *ex parte* filing, provided them with a head start in its public relations campaign.

The All Writs Act. The government requested the order under the authority of the All Writs Act, a 227-year-old law signed by President George Washington himself, as a source of authority for judges to issue orders that are not otherwise covered by a statute.

Tim Cook's Response to the Judge's Order. The issuance of Judge Pym's order prompted Apple CEO Tim Cook to promise to fight the government until the bitter end. "We have great respect for the professionals at the FBI, and we believe their intentions are good," Cook said in an open letter to Apple's customers. "Up to this point, we have done everything that is both within our power and within the law to help them," it continued. "But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."

"Once created," Cook wrote, "the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

"The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers," wrote Cook. "We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data."

Cook asserted that Apple would have to create a "GovtOS," in order to meet the FBI's demands. Apple would also need to create an FBI forensics lab on site that Apple asserts could likely be used to unlock iPhones in the future, which, in public statements, other law enforcement officials have already indicated is likely to follow.

Apple's Motion Opposing the Judge's Order. Apple next filed a motion in opposition to the Judge Pym's order, drafted by a team including the famed appellate lawyer Ted Olson. Apple's essential arguments, now formally codified in their motion, are as follows:

- *The Fifth Amendment's Due Process clause prohibits the government from compelling Apple to create the new version of iOS.*

  "[G]iven the government's boundless interpretation of the All Writs Act, it is hard to conceive of any limits on the orders the government could obtain in the future. For example, if Apple can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user? Nothing;"

- *The government's request to ask Apple to create the new version of iOS, called GovtOS (including coding, signing, verification and testing) is too extraordinary a burden*.

  "No operating system currently exists that can accomplish what the government wants, and any effort to create one will require that Apple write new code, not just disable existing code functionality. Rather, Apple will need to design and implement untested functionality in order to allow the capability to enter passcodes into the device electronically in the manner that the government describes. In addition, Apple would need develop and prepare detailed documentation for the above protocol to enable the FBI to build a brute-force tool that is able to interface with the device to input passcode attempts, or design, develop and prepare documentation for such a tool itself. Further, if the tool is utilized remotely (rather than at a secure Apple facility), Apple will also have to develop procedures to encrypt, validate, and input into the device communications from the FBI. This entire development process would need to be logged and recorded in case Apple's methodology is ever questioned, for example in court by a defense lawyer for anyone charged in relation to the crime. Once created, the operating system would need to go through Apple's quality assurance and security testing process. Apple's software ecosystem is incredibly complicated, and changing one feature of an operating system often has ancillary or unanticipated consequences;"

- *The Order would instantly empower federal, state and local authorities to barrage Apple with demands that will tie up its resources forever.*

  "The government says: 'Just this once' and 'Just this phone.' But the government knows those statements are not true; indeed the government has filed multiple other applications for similar orders, some of which are pending in other courts. And as news of this Court's order broke last week, state and local officials publicly declared their intent to use the proposed operating system to open hundreds of other seized devices—in cases having nothing to do with terrorism. If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent;' and

- *Forcing Apple to write code that weakens its devices and the security of its customers constitutes a violation of free speech as protected by the Constitution.*

> "The government asks this Court to command Apple to write software that will neutralize safety features that Apple has built into the iPhone in response to consumer privacy concerns . . . Under well-settled law, computer code is treated as speech within the meaning of the First Amendment . . . The Supreme Court has made clear that where, as here, the government seeks to compel speech, such action triggers First Amendment protections . . . Compelled speech is a content-based restriction subject to exacting scrutiny. . . . and so may only be upheld if it is narrowly tailored to obtain a compelling state interest."

The Government's Response to Apple's Opposition Motion. The Justice Department issued the following response to Apple's filing:

> "The Justice Department's approach to investigating and prosecuting crimes has remained the same; the change has come in Apple's recent decision to reverse its long-standing cooperation in complying with All Writs Act orders. Law enforcement has a longstanding practice of asking a court to require the assistance of a third-party in effectuating a search warrant. When such requests concern a technological device, we narrowly target our request to apply to the individual device. In each case, a judge must review the relevant information and agree that a third party's assistance is both necessary and reasonable to ensure law enforcement can conduct a court-authorized search."

Other Opinions. The case is politically and legally divisive but in unpredictable ways. Most of the presidential candidates have addressed the issue on the campaign trail. Silicon Valley is split with Microsoft CEO Bill Gates agreeing that the government's request is reasonable and Google and Facebook backing Apple. Interestingly, former NSA Director Michael Hayden, who helped implement the agency's controversial metadata program and still supports it, is in Apple's corner. Even Howard Stern has expressed an opinion. Stern, the wildly popular (and extremely bright) broadcaster offers probably the most interesting, most surprising and most objective opinion of everyone (though his equally sharp sidekick, former Army Captain Robin Quivers, disagrees).

SOME THOUGHTS

The Government's Dubious Legal Theory. First off, the government's citation of the All Writs Act, a colonial statute, to support its motion, raises an immediate red flag. Think about it: The FBI is actually using a law written not just before the era of telephones and computers, but also before the era of *electricity*, to address the encryption of iPhones.

Even more startlingly, the government is actually using a statute enacted just 13 years after the American Revolution to support a unilateral government power that would undermine fundamental principles of the Constitution that *many of in Congress had personally just helped to write or to ratify*. This is an awkward application of statutory construction to say the least – and utterly unconvincing.

Law professors describe the All Writs Act and other similar statutes as laws of so-called "compelled assistance," which are a garbled, confusing and far from settled area of legal jurisprudence.

Although around for over 227 years, case law regarding the 18th Century All Writs Act is actually scant, probably because:

- Most companies lack the resources to battle the government over writs;

- Opposing the government on any kind of subpoena, writ or other demand can further exacerbate an already challenging situation and draw increased and unwanted scrutiny; and

- Refusing to comply with a subpoena or other government request can make it more difficult to win important "cooperation points," which, if charges are filed, can reduce sentences and mitigate other possible punishments.

All Writs Act Precedent *Before Yesterday*. Until yesterday, there were a few scattered reported judicial cases pertaining to the All Writs Act, which were telling and relevant. But yesterday, an All Writs Act case was decided in New York that is spot-on point and will likely have dramatic implications for the Apple/FBI matter. First, let's turn to the cases decided before yesterday's New York case decision:

The first case worthy of mention, which the government cites as support for its motion, is a 1977 case called United States v. New York Telephone Co. In this case, the government used the All Writs Act to obtain a court order forcing a phone company to help set up pen registering devices (designed to record dialed numbers) on two telephones. In that case, there was "probable cause to believe that the company's facilities were being employed to facilitate a criminal enterprise on a continuing basis." Oddly, when carefully considered, this case actually cuts against the government's position.

Compelling Apple to create an entirely new operating system to compromise the privacy of its customers is a far cry from forcing a telephone company to build a system that records a list of numbers dialed by a telephone company customer. Along these lines, Apple easily distinguishes the 1977 case, stating in its opposition motion brief:

> "First, the Court found that the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." Second, the assistance sought was "meager," and as a public utility, the company did not "ha[ve] a substantial interest in not providing assistance. Third, "after an exhaustive search," the FBI was unable to find a suitable location to install its own pen registers without tipping off the targets, and thus there was "no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished" without the company's meager assistance. Applying these factors to this case confirms that the All Writs Act does not permit the Court to compel the unprecedented and unreasonably burdensome assistance that the government seeks."

A 2005 All Writs Act case also worthy of mention, captioned In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and

Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, interestingly stands for the proposition that the All Writs Act has limits.

In that case, New York federal magistrate James Orenstein, ruled that the All Writs Act could not be used to force a phone company to allow real-time tracking of a phone without a warrant, stating:

> "Thus, as far as I can tell, the government proposes that I use the All Writs Act in an entirely unprecedented way. To appreciate just how unprecedented the argument is, it is necessary to recognize that the government need only run this Hail Mary play if its arguments under the electronic surveillance and disclosure statutes fail . . . The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. *Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority*." (emphasis added)

Another more recent 2014 case similarly enunciating the All Writs Act's limitations actually involved Apple and is captioned, "In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant," and was filed just across the bay in federal court in Oakland.

In that case, prosecutors asked a federal judge to "assist in the execution of a federal search warrant by facilitating the unlocking of an iPhone." The government argued that:

> "This court should issue the order because doing so would enable agents to comply with this Court's warrant commanding that [an] iPhone be examined for evidence identified by the warrant . . . Examination of the iPhone without Apple's assistance, if it is possible at all, would require significant resources and may harm the iPhone. Moreover, the order is not likely to place any unreasonable burden on Apple."

In response, Magistrate Judge Kandis Westmore ordered that Apple "provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data." She did not specifically mention the All Writs Act, but she added in her order: "It is further ordered that, to the extent that data on the iOS device is encrypted, Apple may provide a copy of the encrypted data to law enforcement *but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data*. " (emphasis added)

Westmore's language is a near duplicate of a June 6, 2014 order issued by a different California judge in the San Jose division, just 40 miles south of Oakland. There, Magistrate Judge Howard Lloyd ordered Apple to assist in the search of an iPad Mini, months before the release of iOS 8 (which contained the newly enhanced encryption) and again stated in clear and certain terms, "*Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data*."

The Oakland and San Jose matters are also distinguishable from the current Apple/FBI dispute because each involved an older iPhone, which was much simpler and easier to crack

(and did not involve creating a new operating system or removing encryption protections). In fact, no prior case (using the All Writs Act or any other authority) has ever mandated that engineers be conscripted to create a new architecture to defeat a company's own security measures.

All Writs Act Precedent *After Yesterday*. Yesterday, New York Federal Magistrate Judge Orenstein resoundingly reaffirmed his view as to the limitations of the All Writs Act. He is obviously not convinced by the government's position, and seems even a bit outraged by it.

The New York federal case, captioned, In Re Order Requiring Apple, Inc., to Assist in theExecution of a Search Warrant Issued by the Court, held that Apple does not have to help the government unlock a drug dealer's iPhone. In this case, the federal prosecutors in New York sought Apple's assistance in unlocking the password-protected iPhone of Jun Feng, a drug dealer who negotiated a plea late last year. In executing the warrant to search Feng's residence, agents of the United States Drug Enforcement Agency (DEA) properly seized several mobile devices, including Feng's mobile telephone, an iPhone 5s that used Apple's older, less secure, iOS7 for its operating system.

In Judge Orenstein's order, he uses some form of the term "absurd" nine times in rejecting the government's contention that, under the All Writs Act of 1789, the court could require Apple to help in its investigation of a suspect's iPhone. The judge concluded that the AWA does not permit such a reach, and the relief the government seeks is unavailable because "Congress has considered legislation that would achieve the same result but has not adopted it."

Judge Orenstein first notes that the government cannot use the All Writs Act because other statutes apply to the situation – and the All Writs Act can only be elicited when no other statute is relevant to the facts and circumstances of a case. Specifically, Judge Orenstein believes that CALEA, The Communications Assistance for Law Enforcement Act, essentially preempts the government from using the All Writs Act. CALEA is a federal law that enables the government to intercept wire and electronic communications and call-identifying information under certain circumstances -- in particular, when it is necessary in order to protect national security.

Along these lines, Judge Orenstein states, that "it is arguable that CALEA explicitly absolves a company like Apple of any responsibility to provide the assistance the government seeks here and also because even if CALEA does not have such an explicit prohibition, it is part of a larger legislative scheme that is so comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe."

Judge Orenstein also finds that the government is clearly over-reaching under any circumstance. In one particularly scathing portion of his opinion, Judge Orenstein writes: "The implications of the government's position are so far-reaching — both in terms of what it would allow today and what it implies about congressional intent in 1789 — as to produce impermissibly absurd results."

The government also argued that under its interpretation of the All Writs Act, the judge can rule that Apple has to help break into the phone because there is no law saying that Apple

does not have to do so. Judge Orenstein firmly rejects that argument, emphasizing that such an interpretation would make it so that, unless Congress could stop it, the judiciary could make up any rules it wanted.

Judge Orenstein also takes a swipe at the government's use of a 1789 statute to confer powers upon the government that Congress had only, just a few years before, used as a justification for rebellion against British rule. Judge Orenstein states:

> "The government's position also produces a wholly different kind of absurdity: the idea that the First Congress might so thoroughly undermine fundamental principles of the Constitution that many of its members had personally just helped to write or to ratify. Its preferred reading of the law – which allows a court to confer on the executive branch any investigative authority Congress has decided to withhold, so long as it has not affirmatively outlawed it – would transform the AWA from a limited gap-filing statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or preempt. I conclude that the constitutionality of such an interpretation is so doubtful as to render it impermissible as a matter of statutory construction."

One final note, this New York matter involves iOS7, the older operating system that allows for a simpler and less burdensome hacking by Apple. Yet Judge Orenstein still believes that the government is imposing a burden upon Apple that is too high. He writes:

> "[t]he advent of more recent operating systems has done nothing to slow the government's requests – instead, the government continues to seek orders compelling Apple's assistance in bypassing the passcode security of more recent models and operating systems, notwithstanding the fact that such requests are more burdensome than the one pending here."

The Slippery Slope. The crux of the dispute between Apple and the government rests on a fairly straight-forward question: Does the government have the right to review the communications of its citizenry, no matter how tightly the communications are sealed and encrypted; no matter how onerous the burden on the company to crack its own security; and no matter how strict and narrow a standard is applied to the government's request or demand.

Apple's argument in this regard makes a lot of sense. Seeking a writ to enlist Apple to create a new operating system creates a fairly dangerous slippery slope. Consider future possibilities such as Writs ordering:

- Apple to create programs to track secretly the location of suspects, or secretly use the iPhone's microphone and camera to record sound and video;
- Google to create proprietary algorithms to track suspicious Internet searches;
- Facebook to engage Palantyr to develop behavioral data analytics software to identify users who may pose a threat to the security of the United States;

- SnapChat (the popular mobile app that allows for the sending of videos and pictures, which will self destruct a few seconds after being viewed) to build a virtual warehouse of any suspicious videos or photos; or
- A drug maker to supply lethal injection drugs notwithstanding the manufacturer's conscientious objection to capital punishment.

FBI Director Comey asserts that this order is essentially a "one-off" and will not trigger the kind of cavalcade of demands cited above. Even though Director Comey is probably the most honest, ethical and heroic attorney general in U.S history, some less scrupulous or more aggressive local, state and/or federal investigators are bound to usurp the ruling against Apple and push the edges of the envelope.

The Government Can Never Prevent People From Communicating Outside of Governmental Purview. Regardless of the validity of the legal theories presented by either side of the dispute, some commentators assert that the primary societal issue presented by the Apple/FBI conflict is: *Should* the government have the right to review (under any standard) the communications of its citizenry, no matter how tightly they are sealed and encrypted.

The government's position, for example, as articulated by the National District Attorneys Association, is that "no house is permitted to be made impervious to search by a lawfully issued warrant reviewed by a neutral magistrate and based upon probable cause, and no technology company should be able to distribute telephones in America that cannot be legally accessed by law enforcement conducting a criminal investigation after judicial review and issuance of a lawful order,"

This position is outdated and unrealistic to say the least. Historically, governmental access to communications between individuals was as simple as a wiretap or mail-intercept, and was available to the government upon application to a judge, and a proper showing of probable cause, particularity and the rest. But those days are gone forever.

Nowadays, opportunities for secret communications between people abound, with little chance (if any) of governmental intercept. Consider steganography apps (of which there are many), which allow users to embed hidden messages inside what appear to be family photos or audio files, with limited coding and in such a manner that it is almost impossible to detect. In the world of cryptology, a secret code known only to the user usually means that the information could be kept away from the government unless there is an existing means to compel the person to reveal it.

Besides being obsolete, the question presented is actually moot. Because even if the government were to pass a law banning fully encrypted communications, terrorists would invent other ways to mask their communications, or more likely, would simply ignore the encryption ban, just like terrorists ignore the laws against murder. Given the technological age we live in, there are, and will always be, endless technological ways to disguise interpersonal communications.

Indeed, this growing limitation upon government surveillance is not news to the FBI. The FBI began sounding alarms years ago about technology that allowed people to exchange private

messages protected by unbreakable encryption. The N.Y. Times reports that in fall 2010, at the behest of then FBI Director Robert S. Mueller III, the Obama administration began work on a law that required technology companies to provide unencrypted data to the government. Lawyers at the FBI, DOJ and Commerce Department drafted bills around the idea that technology companies in the Internet age should be bound by the same rules as phone companies, which were forced during the Clinton administration to build digital networks that government agents could tap.

"Supporting Apple Means Supporting Terrorists" is an Unfair Edict. This notion, that American citizens must support the government's demand of Apple, otherwise terrorists will be able to communicate free from surveillance, is misguided and designed to trigger emotion and obfuscate legal analysis. Whether or not Apple is forced to construct a new operating system, terrorists will always have ways to communicate in secret and without the fear of government surveillance. And even if nations went so far as to somehow mandate backdoors, there will always be some encrypted channels outside of their jurisdiction where the likes of ISIS can plot.

Lets also remember that there will also always be legitimate needs for encrypted communications. Just ask Chinese pastors, North Korean protestors or Russian dissidents who are targeted by authoritarian regimes, want to communicate with one another and require encryption to do so (if they want to avoid getting jailed or even killed).

Apple is also entitled to the same freedoms as everyone else. As Judge Orenstein notes in yesterdays New York decision, when the government argues that Apple should be a good citizen and comply:

> "Such argument reflects poorly on a government that exists in part to safeguard the freedom of its citizens – acting as individuals or through the organizations they create – to make autonomous choices about how best to balance societal and private interests in going about their lives and their businesses. The same argument could be used to condemn with equal force any citizen's chosen form of dissent. All American citizens and companies 'derive significant legal, infrastructural, and political benefits from their status as such' – but that cannot mean that they are not burdened in a legally cognizable way when forced unwillingly to comply with what they sincerely believe to be an unlawful government intrusion."

Privacy is Something Americans Take Very Seriously. We live in a society where technology could empower the government to pummel traditional privacy barriers and reduce crime exponentially. For instance, the government could:

- Require identity cards be carried by all residents and citizens;
- Register everyone's DNA with the government on the day they are born;
- Require registration of every single phone used (just like with cars);
- Require continuous geolocation devices in every car and mobile phone;

- Install video cameras on every street corner;
- Prohibit the manufacture and use of disposable mobile phones; and
- The list goes on.

Our society has decided however, that privacy intrusions like those cited above are not palatable. Whether young, old, Republican, Democrat northerner, southerner, etc., every constituency shares common ground when it comes to government snooping. All are suspicious, skeptical and apprehensive.

Perhaps in this new era of such horrific terrorism, and where social media has opened up the personal lives of so many people, there exists less concern about privacy. It is tough to tell. What is so interesting and yet another strange and unexpected irony that further clouds the debate, is the fact that young people are rallying so passionately behind Apple. Yes, the same generation whose use of social media has exposed their private lives in ways their parents and grandparents could never even have imagined, seems passionate about Apple's efforts to protect their personal privacy.

Technology Has Empowered the Government in Extraordinary Ways and the Government Must be Kept in Check. Historically, logistical concerns, rather than legal constraints, hindered the government's use of overbroad subpoenas, requests and search warrants. For instance, an overbroad DOJ subpoena could result in a company's "backing up the truck" to DOJ headquarters and dumping hundreds or even thousands of boxes of documents in response. Overbroad subpoenas before computers were a logistical nightmare, not just to review, but even to inventory, manage and warehouse, causing lengthy and tedious investigation delays.

But those days are long gone. Subpoena responses that used to require rooms, floors and buildings to store, and legions of agents to review, now merely require a silicon microchip for their storage and one agent to analyze (using an e-discovery tool). Document reviews that used to take months now take hours, even minutes.

Technology has clearly transformed the investigative playing field, empowering the government in groundbreaking and pioneering ways to identify, pinpoint, examine, segregate, and peruse data. To its credit, when it comes to data and the ever-elusive smoking gun, the government has become more creative, more resourceful (and more effective) than ever. *But merely because technology can facilitate an investigative outcome does not automatically mean there exists authority to do so.*

For example, consider the SEC investigatory assertiveness. Despite clearly lacking the authority to do so, the SEC's enforcement arm issues subpoenas for the production of so-called "electronic storage devices" (ESDs) such as hard drives, mobile phones, tablets, etc. – and no one in government seems to care.

The SEC is, of course, an exceptional federal government agency -- staffed with a dedicated corps of highly-credentialed professionals, inspired by a noble sense of mission, and rich with an 80+ year history of investor advocacy. But sometimes the SEC gets carried away and

needs a quick reality check. This is the case with the SEC's use of subpoenas demanding production from witnesses of their ESDs. Yet, until someone like Tim Cook comes along and says, "stop," the improper and unauthorized SEC practice will unfortunately continue.

A Legislative Solution is Unlikely. In its opposition motion, Apple argues that upholding the Judge's order "would preempt decisions that should be left to the will of the people through laws passed by Congress and signed by the President." Apple cites the FBI Director himself to support this proposition:

> "FBI Director James Comey expressly recognized: Democracies resolve such tensions through robust debate. . . . It may be that, as a people, we decide the benefits [of strong encryption] outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in the world of universal strong encryption. Those are decisions Americans should make, but I think part of my job is [to] make sure the debate is informed by a reasonable understanding of the costs."

Apple further notes, that:

> "The government, by seeking an order mandating that Apple create software to destabilize the security of the iPhone and the law-abiding citizens who use it to store data touching on every facet of their private lives, is not acting to inform or contribute to the debate; it is seeking to avoid it."

This aspect of the arguments of both Apple and the FBI misses the mark. Most laws pertaining to the private communications between American citizens (perhaps with the exception of the USA Patriot Act, which was hastily passed after 9/11), protect privacy and limit the kind of private data that government investigators can access. For instance, laws such as The Privacy Act of 1974, the Electronic Communications Privacy Act of 1986 (ECPA), the Cable Communications Policy Act of 1984, and The Right to Financial Privacy Act of 1978 all curtail government authority and affirmatively protect the privacy rights of individual American citizens.

This brings to mind a 1998 ECPA case during the time of "don't ask, don't tell," involving a highly decorated gay Naval sailor by the name of Timothy R. McVeigh, who was the senior-most enlisted man aboard the U.S. nuclear submarine U.S.S. Chicago.

While in Honolulu, McVeigh sent email messages from his America Online (AOL) account using the screen name "boysrch" and the signature "Tim," when communicating with a civilian working as a volunteer on a Navy-sponsored charity. The AOL user directory identified the marital status of the owner of the "boysrch" account as "gay." Someone tipped off naval authorities about the AOL account, which launched an investigation.

A Navy paralegal called AOL seeking the identity of "boysrch." The paralegal did not identify himself as a Navy official and did not follow the ECPA's requirement that, among other things, government officials, in order to obtain information from AOL, must either: 1) obtain a warrant; or 2) notify the subscriber and issue a subpoena.

AOL provided the information to the Navy and McVeigh was dishonorably discharged for violating the "don't ask, don't tell" rule. McVeigh sued and the case soon made its way into the D.C. federal courtroom of Judge Stanley Sporkin, the celebrated former SEC Enforcement Director and former CIA General Counsel, who was very disturbed by the Navy's position. The Navy actually admitted violating the ECPA; however, the Navy argued that AOL was at fault because AOL provided the information to the Navy and should not have done so.

Judge Sporkin's outrage back then resonates just as loudly today, when he wrote in his opinion,

> "In these days of 'Big Brother,' where through technology and otherwise, the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights are strictly observed."

Congress will find it challenging to turn the tides against historical notions of privacy protection. Americans might instinctively favor the government's position against Apple – after all, what American wants to defend the rights of murdering terrorists? But when push comes to shove, American citizens are loath to sacrifice their privacy and become suspicious of an aggressively prying government, and American judges like Judge Sporkin are equally distrustful.

The Impact of the Release of Apple's Code-Breaking Operating System. Apple asserts that if it were to create an operating system that would allow brute-force attacks, the new software would find its way into the wrong hands. The government claims that Apple is perfectly capable of protecting the new operating system, just like any other trade secret. While both the intended and unintended consequences of scenarios like destabilizing encryption of smart devices are difficult to predict, one thing is for certain. The moment any company builds a backdoor for use by governments, it will only be a matter of time before hackers figure it out and coopt it.

The government also makes a puzzling argument that the order only impacts *one phone*. But it seems that there does not exist a "single phone option." Given that Apple is bypassing a core function of the iPhone's operating system, it seems technologically infeasible for Apple to build that option to work with just one sole phone. The government is asking Apple to remove the restriction that wipes the iPhone after 10 tries, and that option is the same on every iPhone.

CONCLUSION

Having worked as an investigator/prosecutor for almost 20 years, including 11 years as Chief of the SEC's Office of Internet Enforcement, and having drafted the online investigative guidelines that the SEC Enforcement Division used during my tenure, I trained a legion of lawyers and investigators how to manage (and balance) the many privacy concerns of Americans.

In crafting the calculus to factor into the breadth and scope of government subpoenas, demands and requests, my lesson encouraged the asking of four questions before seeking any information of any kind:

- Is the information available elsewhere? That is, perhaps the information was produced by another witness or is available in some public place;

- Is it lawful to obtain the information? That is, does the investigative subpoena pass muster under the litany of privacy protection statutes, rules and regulations;

- Is the information request or demand "fishing?" That is, can the government articulate with particularity the nature of the information sought or does it just "feel like" there may exist something interesting in the information requested or demanded; and

- Is it right to subpoena this information? This is perhaps the most important question of all. The answer to this last question varies with societal mores and is a question that the director of every law-enforcement agency must ponder carefully when constructing guidelines, especially because, as Dragline said to "Society" in Cool Hand Luke, "When it comes to the law, nothing is understood."

Good prosecutors and agents always ask some iteration of these four questions before demanding information from witnesses, subjects or targets, of investigations. Whether the government investigators who sought the order from Apple asked them all is not clear (though, despite having the best of intentions, they probably did not).

There may indeed be some middle ground between Apple and the FBI, although the situation seems bleak for any sort of compromise, especially given the government's *ex parte* approach to negotiation, which really ratcheted up the disagreement's intensity.

The dispute between the parties brings to mind perhaps the most well known quote from Cool Hand Luke; this time from the prison warden, who has become increasingly frustrated with Luke's rebellious ways, and forces the imprisoned Luke to wear chains on his legs. When explaining his extreme position concerning Luke to the rest of the chain gang, the warden states authoritatively:

"What we've got here . . . is a failure to communicate."

Failure to communicate is an understatement when considering the Apple/FBI relationship; but there is always hope. For the government, there is hope that the public pressure on Apple will prompt a settlement of some sort. For Apple, there is a hope that an appellant court will, among other things, reverse such a broad, unwieldy and extreme application of the All Writs Act.

I would bet my money on Apple, just like I would have bet my money on Luke and Dragline (if I were an esteemed member in good standing of their chain gang). As Judge Orenstein wrote in his recent opinion:

> "In deciding this motion, I offer no opinion as to whether, in the circumstances of this case or others, the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate societal interests arrayed against it here. Those competing values extend beyond the

individual's interest in vindicating reasonable expectations of privacy . . . They include the commercial interest in conducting a lawful business as its owners deem most productive, free of potentially harmful government intrusion; and the far more fundamental and universal interest – important to individuals as a matter of safety, to businesses as a matter of competitive fairness, and to society as a whole as a matter of national security – in shielding sensitive electronically stored data from the myriad harms, great and small, that unauthorized access and misuse can cause.

How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive. It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789."