"This is the discussion of the era, and this book is smack in the middle of it."
— JON STEWART, *The Daily Show*

PRIVACY IN THE AGE OF BIG DATA

RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY

THERESA M. PAYTON AND THEODORE CLAYPOOLE

Foreword by Hon. Howard A. Schmidt

6

THE SPY IN YOUR POCKET

The power, convenience, and plain fun of our smartphones and tablets turn them into constant companions. And that means, whether you know it or not, that you just might just have a spy in your pocket. There is no question that the miniature computers we carry around with us enhance our lives in many ways. However, indiscriminate and careless use of the technology can ruin your privacy, as criminals, corporations, police, and even hostile governments fill their files about you with intimate information about where you go and what you do.

By understanding what data is being captured by your mobile devices and who is using that information, you can better control how your life is monitored and what others know about you.

JOHN MCAFEE AND THE SECRET LOCATION

John McAfee is a pioneer in Internet security and a Silicon Valley legend. A highly sophisticated programmer and businessman, McAfee created the antivirus program and company that still bear his name. He sold his remaining stake in this company in the 1990s, two years after it went public. But McAfee is known as much for peculiar behavior as business and technology acumen. A former cocaine dealer who later took out newspaper ads discouraging drug use,[1] he has taught yoga and published yoga books, collected guns and ammunition, and lived with eight women at a time.

By 2009, McAfee had sold off nearly all his major holdings, including estates in Hawaii, Texas, New Mexico, and Colorado. He moved into the jungle in Belize, a small country located on the northeastern coast of Central America. There McAfee started a new venture called QuoremEx, which was founded to produce commercial antibiotics. Living in the jungle brought McAfee closer to the wild in more ways than one. He wrote to friends, "My fragile connection with the world of polite society has, without a doubt, been severed. My attire would rank me among the worst-dressed Tijuana panhandlers. My hygiene is no better."[2]

McAfee argued with his neighbor, Greg Faull, about McAfee's eleven dogs and the noise they made. Faull filed police reports and threatened to shoot the dogs. On November 9, 2012, McAfee's dogs were poisoned and died. Two days later, Greg Faull was found lying in a pool of blood, shot execution style. When the Belizean police arrive at McAfee's house to question him about the murder, McAfee dug a shallow trench and buried himself for hours.[3] Then he disappeared.

Wanted in Belize for questioning in the murder of Greg Faull, McAfee went into hiding. He claimed to be innocent of the murder; however, from previous experience in a Belizean jail, he also feared for his life in the hands of the police. The international press speculated for weeks on the whereabouts of the eccentric software tycoon. Authorities were stymied. Then all the speculation came to an end thanks to data captured by a cell phone.

McAfee agreed to meet with journalists at a secret location. During the meeting, one of the journalists took McAfee's picture with his smartphone camera. He posted the image on the Internet with the caption, "We are with John McAfee right now, suckers."[4]

Apparently, neither the journalist nor McAfee realized that nearly all smartphone pictures include metadata—information about the picture itself—contained in the same file as the photograph. The journalist's cell phone captured data relating to the time the picture was taken and the exact global coordinates where it was taken. When a cell phone picture is posted on the Internet, its metadata can be examined by anyone who has the right tools. In the case of John McAfee, a hacker called Simple Nomad examined the metadata and promptly published his finding that "McAfee's image emanated from an iPhone 4S at the following location: 'Latitude/longitude: 15 39' 29.4 north, 88 59' 31.8 west' at 12:26pm Monday.'"[5] McAfee was quickly traced to a Guatemalan villa.

On December 5, 2012, Guatemalan police arrested John McAfee for illegally entering the country. A week later, he was deported to the United States.[6] If a paranoid programming master like John McAfee, while hiding from the police and in fear of his life, can lose his valuable privacy because of the extensive data capture and reporting from smartphones, what chance of privacy do the rest of us have? We carry this spy in our pockets that sends out a steady stream of information about us. The only way to stop the cell phone's reporting is to remove its battery, but many models make battery removal impossible. The smartphone may be the most significant threat to the private information that matters the most to you.

WHAT INFORMATION DO MODERN SMARTPHONES CAPTURE?

Your authors are old enough to remember when beepers were the most effective mobile-communication device available to the general public. Although beepers could only send and receive a short text message, they became the pocketknife of the 1980s, providing a single-function tool that easily fit in your pocket or purse. In comparison, today's smartphones are the ultimate Swiss-army knife of electronics, providing an array of diverse tools in pocket-friendly form. Smartphones are full computers, capable of managing an entire office, accessing documents and video online, and acting as a mail server and text message machine. Your smartphone can replace your camera, watch, and compass while providing maps and directions for travel. It has full browser capability with hundreds of thousands of mobile apps that help you find a taxi, provide a flashlight in the dark, or fling colorful angry birds at elaborately constructed pig shelters. Oh yes, and it makes telephone calls from nearly everywhere.

But this amazing power comes at a significant cost. While the price of a two-year cell and data plan is expensive enough, the cost to your privacy is astronomical. To understand why, we look at the flexible toolset contained in a modern smartphone to see what information it is capturing around you. In the process, we discover that it's the way two or more of these data-capture tools *work together* that helps not only you in your mobile life but also marketers, thieves, law enforcement, and anyone else who wants access to detailed information about you. Remember, John McAfee could be betrayed

by a posted picture first because the journalist's device was capable of taking a digital picture, and then because the device noted the time and exact global location that the picture was taken.

The same handheld technology was used to help identify the bombing suspects at the 2013 Boston Marathon,[7] as dozens of crowd participants at Copley Square uploaded time-stamped and location-stamped photographs to the FBI's website. Combining the smartphone's camera with a clock and Global Positioning System (GPS) sensors provided useful, detailed information that would likely hold up in court.

A Variety of Location Sensors

Let's start with the location functions of a smartphone. As you would suspect, your smartphone's location at any given time can be tracked using its GPS locator. This highly accurate location device taps into the satellite-based global positioning system that was opened to nonmilitary uses during the Clinton administration, enabling your cell phone to talk to satellites to determine its location. This information is likely recorded by many applications of your phone, as well as by law enforcement or your phone's software or hardware makers if they are interested.

Though most smartphones permit you to turn the GPS feature on and off, the GPS feature is not necessarily the only locator on your phone. For example, some smartphones come preloaded with weather applications that continually ping the satellites, a process that also provides information about the phone's location.

Your phone is also talking to cell towers. Even before the introduction of GPS sensors, a cell phone's location could be determined by triangulation among cell towers. A cell phone access provider can pinpoint the location of your call by bouncing the signal off the closest three cell towers and determining your position between them. By comparing the relative strength of your phone's signal to multiple antennae towers, a tracker can determine a rough location for the device. Using your phone on the move makes this calculation easier because it provides a stream of data points as you move into the range of one cell tower and out of the range of another. In the United States, phone providers receive thousands of requests each day from law enforcement for cell-tower-triangulation data. This method of tracking is popular in part because, though many smartphone users can turn off the GPS-signaling device on the smart-

phone, they are unable to stop the phone from continuing to ping cell towers. Your phone is still reporting its location as long as the batteries are powering the device.

If your smartphone seeks out *Wi-Fi* networks, then it also can be tracked by which Wi-Fi networks it picks up. Wi-Fi is a term for wireless local area network using a common standard for interoperability. Wi-Fi networks are everywhere: they are business networks, home wireless routers, and even some are government-sponsored, free wireless connectivity. So as you pass a Starbucks, your phone may ping its network, telling the phone carrier that you are in that location at a certain time. Bluetooth signals can make your phone vulnerable to tracking, but only to those within close proximity.

Some hybrid methods of smartphone tracking combine these methods of locating a phone to pinpoint location. For example, Apple uses messages on the iPhone encouraging its iPhone users to turn on Wi-Fi-locating signals to help refine mapping functions. The more of these functions you keep on and available, the tighter the circle your phone company and location app providers can use to pinpoint your location.

In addition to the built-in trackers, you could allow everyone to track your location by signing up for a mobile application that facilitates tracking and broadcasts your location. Google Latitudes allows friends or relatives to connect online and see each other's smartphone location as they travel. Foursquare is a game application that uses your location in the real world to earn points, badges, and status in the game, allowing you to become "Mayor" of your local deli if you visit enough times. There are even dating applications that show you the number of interested people in your vicinity who share or complement your dating preferences, so you can find each other right away. The tradeoff is that people using the application can see when they are close to you and can read your interests as they watch you from across the room.

Touch, Voice, and Image Sensors

In addition to GPS, Wi-Fi, and cell tower signaling/sensing devices, the current smartphone is packed with sensory equipment for detecting touch, sound, and images. Its primary input sensors are the touch screen and the microphone. Early smartphones used only touch screens to choose which apps you wish to run and which emails you want to read; today, many

smartphones are also responsive to your voice and some to the wave of your hand.

On October 4, 2011, Apple introduced the Siri voice-activated personal-assistant system to its phones, and applications such as Dragon Dictation and Google Voice provide vocal interfaces into performing smartphone tasks. Smartphone manufacturers are poised to build more functionality with a voice interface as the technology becomes easier to use. Touch screens and microphones on smartphones could be used to test our health by reading pressure exerted by our fingers or the strength and inflections of our voice. Microphones can serve as biometric identifiers to authenticate your identity and authorize transactions, recording your voice and comparing it to earlier samples. The microphone can listen in and record conversations, not just over the telephone lines, but any conversation within the sensitivity range of our smartphones.

Smartphones also sense and collect images. Most smartphones sold today have two cameras, one in the back for taking pictures and video of your surroundings, and one on the front to allow you to Skype, Snapchat, or videoconference with other people, so that you can see each other's faces as you interact. Phone-front cameras could one day allow screen scrolling by watching eye movement or air gestures you make with your hands or head. Cell phone cameras are changing the face of photography, news reporting, law enforcement, and society, since many of the witnesses to unusual scenes can document on video what used to be simply described in firsthand accounts.

However, when you have a computer connected to the Internet, it is possible for someone you don't know to turn on your computer's camera or its microphone to sense where you are and what you are doing at any time. Though it takes sophisticated malicious software to do this in a sneaky fashion, it certainly is possible for law enforcement, a foreign government, or a prospective thief to listen into your life even if you thought your smartphone was inactive. This is what happens when you carry a remotely driven camera and microphone with you all the time.

Utility Sensors

Your handheld computer may also contain an accelerometer, magnetometer (compass), barometer, proximity sensor, light sensor, and a gyroscope. Any of these device-based sensors can be accessed by applications that you

download or which come preloaded on your device. They can be used to sense how fast and which direction your device is moving at a given time (which often translates into how fast and where you are moving), what the weather many be in the vicinity of your smartphone, and whether the phone is in your purse or out in the sun.

As more applications are built to take advantage of these sensors, they can gather more information to tell more about your activities, habits, and locations. Fordham University has established a Wireless Sensor Data Mining Lab, concerned with collecting the sensor data from mobile devices and analyzing the data recovered for useful knowledge. The Lab has already determined how to biometrically identify a user from accelerometer data, and it has used the smartphone accelerometer to determine if its user is sitting, standing, lying down, walking, or running.

You never know how these apparently benign sensors can be used to mine information about you. For example, the accelerometer measures movement of a cell phone in space, and it is generally used to control video race cars and other game movements. However, Dr. Adam Aviv, working at Swarthmore College, was able to use the phone's accelerometer to determine where the phone's user was tapping on a screen to unlock the device with a passphrase. Simply by reading the internal accelerometer and measuring the phone's movements, Dr. Aviv's software for attacking smartphones was able to identify the correct PIN entered by a smartphone user 43 percent of the time and patterns entered by a user close to 73 percent of the time.[8] This system of attack was hindered when passwords or patterns were entered on the move. So use of the less well-known sensors, alone or in conjunction with others, may lead to information that can intrude deeply on your privacy—including learning your passwords.

In the future we can also expect an expanded set of sensors in our mobile technology. For example, adding altimeters will mean that apps can determine elevation changes for fitness measurements and could determine what floor the user is standing on inside a building, making for more useful indoor maps of museums and sports arenas. This could also help fire or police responders trying to find a person in need of medical attention who signaled for help. Apple has filed for various patents that may signal what device sensors are likely to be in use over the next few years, including a "smart garment" patent that involves clothing that can transmit location and body data wirelessly to an external data-processing device such as an iPhone or iPad.[9] Apple has received patents for an

activity monitor for tracking acceleration, and an earbud that measures a user's blood oxygen level, body temperature, and heart rate. These Apple sensors suggest that the future of mobile technology will include tying your current device into your clothing and other wearable items to give detailed health data through your smartphone.

Business Data Capture

Each transaction you conduct on your mobile device sends extensive data out to many businesses. Each of these companies takes your data and may save it to combine it with more data later in order to build a more accurate picture of your preferences and buying habits. The businesses that are interested in your location can make detailed maps of where you travel, how long you stay at each location, and what you do there. They can combine web-surfing data like any other Internet company, with geolocation data and data from any or all of the other sensors contained on your mobile device. This allows businesses taking your information to add entirely new layers to their knowledge base about you and your behavior.

Each transaction you undertake on your mobile device provides a set of information to a group of businesses that each claim ownership of your data. If you use a mobile sales app to buy shoes from Zappos or another online clothing store, then of course the shoe store gathers and keeps your information. They may try to capture where you were when you made your purchase, but you would have to include your name, address, and payment information to complete the transaction, and probably also include an email address. The shoe company will keep all of this information.

But your telephone company may also register that you made a purchase from your mobile phone. Some telephone companies even offer to allow certain online purchases to be credited to your telephone bill, giving them more information. It is likely that the company who operates the smartphone software ecosystem for your device will also take information regarding your use of the retail app and your purchase. So will the app provider if it is different from the retail store. It is likely that the app will use a separate payment processor, which will also hold some of your data, as will your bank, and the merchant bank for the company that made the sale. Some of these companies can take data directly from your phone during the purchase

and others can't, but they all know more about you after your mobile purchase than they knew before.

MOBILE DEVICES AND EMPLOYMENT

If your company allows or encourages you to access work documents on your personal phone, or to tend to personal business on your work-issued phone or tablet, you should be aware that the company may gain rights to the personal correspondence, pictures, and other data kept on your device. For that reason, using your smartphone for work and granting employer access can severely limit your privacy.

Many of us use our smartphones or tablet computers for work, reading email, revising documents, texting coworkers, attending meetings by videoconference and otherwise operating our entire business lives within the device. In some cases, an employer may provide mobile technology for its sales team or all employees. In others, you are expected to bring your own device to work. In either circumstance, the company may have rights over the data in the smartphone or tablet simply due to its dual use as a personal and business tool. Many businesses will install software on their worker's mobile devices that allows the business to access information from the device, and some companies use software that can wipe all data from the device when it is believed to be lost or stolen.

More employers are starting to adopt "Bring Your Own Device" (BYOD) policies and procedures. You should ask your employer how your personal data will be treated on the mobile device, and ask to see any formal policies affecting your mobile data. Many employers who adopt BYOD policies also provide information technology service assistance to employees, helping with problems, but also allowing the tech professionals from the office to see what personal apps and information you keep on your phone. The closer you tie your private mobile phone to your work, the more likely that your privacy will be lost to coworkers, bosses, and the company's information technology professionals.

In addition, your privacy can disappear quickly when you carry a machine that is relevant to a business court case. If you maintain work-related text messages or email on your smartphone or tablet, or if you keep work-related notes and documents on these devices, then those devices could be tagged as important evidence in a court case against your employer. In

that case, the device could be taken and held in a safe place until it was examined for relevant data by a team of lawyers. Or, its significant data stores could be mirrored on another hard drive and reviewed by the court. Either way, groups of people related to the court case would have access to the information on your device, probably including at least some of your personal information. Furthermore, data from your device could become part of the litigation, read aloud in court, or otherwise exposed in a public forum, such as court or a legislative or administrative hearing. Keeping your personal device completely separate from your business life may be the only way to assure you can avoid this fate.

"MY PHONE HAS BEEN HACKED!"

Given all of the personal information on your smartphone or tablet, the device can be a target for hackers. Anyone watching the news in 2012 heard about the efforts of certain British tabloids to hack into the telephone voice mail of citizens that reporters believed to be newsworthy, and the arrests of reporters and editors that followed the original news stories. One of the oldest British tabloids, *News of the World*, closed itself down due to the ensuing scandal. The privacy of both celebrities and average British citizens was compromised, as reporters were authorized by leaders of News Corporation to hack into the voice mail of deceased British soldiers, victims of the London bombings, and even murdered schoolgirl Milly Dowler. A public outcry and police investigation made it clear that the British citizenry valued its privacy and found such phone-hacking tactics to be unacceptable.[10]

Criminal Hackers

Smartphones and tablets are targets for more than the tabloid press. As more valuable information is stored on or accessed from mobile computers, hackers develop more sophisticated tools to pry into these mobile devices. Juniper Networks noted in its 2011 *Mobile Security Report* that 2011 saw an unprecedented 155 percent increase in mobile malware attacks across all platforms.[11] Juniper also noted "a new level of sophistication of many attacks. Malware writers used new and novel ways to exploit vulnerabilities," such as DroidKungFu using encrypted payloads to avoid detection and

DroidDream disguising itself as a legitimate application. As Google's Android phones grew to become the most popular platform in the world, hackers followed, writing more attacks for the phones operating on Android. Reports have been released showing that Apple phones also have dozens of features vulnerable to hackers.[12]

One of the most destructive hacking tools used against smartphones is a virus called NotCompatible, which allows hackers to take full control of a smartphone. A data security company called Lookout claims that ten thousand customers per day were being tricked into loading the virus on their phones. The virus uses spam to propagate itself, using a contact list method so the messages appear as if they came from someone you know.[13] Once hackers have control of your phone, they can shut down its functionality, take your information, or use the phone for their own purposes. For example, a hacker could force your phone to send out more spam to other phones, just to increase the number of devices under the hacker's control. Or a hacker can make money by forcing your phone to go to pay sites that bill your phone and pay the hacker for each visit. Of course, with information gathered from your smartphone, a hacker could drain your bank account or use your credit/debit card for purchases.

Bluetooth Signals

A smartphone will likely contain a Bluetooth signaler/sensor so that it can communicate with nearby Bluetooth-enabled devices, such as speakers for your music, printers for your documents, and hands-free automobile cockpits for your conversations while driving. The Bluetooth technology was developed to encourage security and interoperability between devices, but it has been shown to be vulnerable to both malicious attacks and to government intrusion. Bluetooth ranges are usually about thirty feet between devices to remain connected. For that reason, Bluetooth hacking is not practical on a large scale because the hacker needs to remain in close proximity to the victim during the attack.

Some of the most annoying Bluetooth vulnerability involves "Bluejacking," or sending messages, including text, video, and audio, to other devices using the Bluetooth connection. Most of the Bluejacking is currently aimed at sending spam-like marketing messages or pranks, although it could be used to transmit more malicious signals such as Trojan viruses.

"Bluesnarfing" is more dangerous and is defined as theft of information from a device through a Bluetooth connection. Bluesnarfing can target calendar information, texts, email, contact lists, and even pictures stored on your smartphone. Some brands of smartphone are known to be especially vulnerable to being hacked in a Bluesnarfing attack, so you may want to investigate this issue before you buy.

"Bluebugging," which can affect both smartphones and Bluetooth headsets, allows a skilled hacker to take control of certain aspects of a smartphone, and even to eavesdrop on a caller's conversations.

But the bad guys are not the only ones exploiting Bluetooth sensors on your phone. The US Transportation Safety Board (TSB) has announced and tested a plan called Automated Wait Time monitoring, which works by "detecting signals broadcast to the public by individual devices and calculating a wait time as the signal passes sensors positioned to cover the area in which passengers may wait in line."[14] So the TSB was capturing the Bluetooth signals emitted by cell phones to monitor passengers' time waiting in security lines.

You can shut off Bluetooth signals by setting your Bluetooth signal to "nondiscoverable." You should never pair your Bluetooth connection with unknown devices.

Government Intrusion

Governments are also believed to hack into smartphones. In May 2013, the Dutch government presented a bill in its legislature to grant permission to law enforcement to hack into computer systems, allowing the Dutch police to block access to child pornography, read the emails of criminals, and track suspects through the GPS signals on their cell phones.[15] But the Dutch government is an open democracy, so it must publically announce how it chooses to address hacking into mobile computing.

In contrast, the Russian and Chinese governments have no such commitments to openness. A recent *Forbes* article proposes that the Chinese government has created a virus specifically targeted at Android phones, and that the virus uses cell-tower triangulation to report the phone's location.[16] The article cites, among other sources, a Canadian human interest group from the University of Toronto who demonstrated that Tibetan activists are being targeted with sophisticated malware designed to infect

Probably Citizen Lab.

Android phones, stealing the phone user's contacts and messages and tracking the phone user's location. "We don't have a smoking gun that this is the Chinese government. But let's face it," says [the group's director Ron] Deibert. "When you add it all up, there's really only one kind of organization for whom this information is useful. And we know that the Chinese have a very strong interest in tracking Tibetans, so it's a strong set of circumstantial evidence."[17]

This report is just one of many implicating the Chinese government of sponsoring hacking attacks, but it is one of the first to identify smartphones as the specific target of the Chinese government.

Not only Tibetans and Chinese political dissidents need to be concerned with government malware. The Chinese government is apparently also interested in the mobile computers of North American businesspeople and government officials. According to Joel F. Brenner, formerly the top counterintelligence official in the office of the director of national intelligence: "If a company has significant intellectual property that the Chinese and Russians are interested in, and you go over there with mobile devices, your devices will get penetrated."[18]

While both Russia and China demand that no one can enter their countries with encrypted mobile devices without government permission to use that encryption, business and government travelers are generally warned that their devices will be hacked upon entering China or Russia. In recent testimony before Congress, James Clapper, the United States' director of national intelligence, stated that the governments of Russia and China were responsible for illicit intrusions into US computer networks and theft of US intellectual property.[19] Computer experts throughout Europe and North America believe that this hacking extends to any Western mobile computer brought within their jurisdiction. Some American companies prohibit their employees from bringing company computers to China, and they demand to inspect the smartphones of anyone who visited China with their devices.[20] When the government is a coercive police state, expect that it will take steps to examine all information from visitors, including the information on your smartphone or tablet.

Governments also intrude on the privacy of other governments through their technology. The US government has been expanding resources to protect its own computers from hacks by foreign powers. In April of 2013, President Obama proposed his second large increase in a row for building a

team of cyberdefenders at the Pentagon. This is in conjunction with increases in funds marked for cyber defense in other cabinet-level organizations such as the Justice Department and the Energy Department. This follows the Department of Homeland Security's announcement that it was looking to hire at least six hundred hackers to improve the department's cyberattack and defense capabilities. Since mobile computers are crucial to government and business, and also highly vulnerable to attack, we can assume some of these resources will be allotted to both protecting and attacking mobile devices.

Law enforcement within the United States is also an increasingly heavy user of information taken from private mobile devices. In July 2012, Congress asked cell phone carriers to report on law-enforcement requests for information on mobile phone customers. The carriers reported receiving 1.3 million law-enforcement demands for subscriber information in the previous year.[21] These requests included text messages and caller locations. Some of the requests included "cell tower dumps" in which the police request the names and numbers of everyone who has been in the vicinity of certain cell towers on a specific day, which could involve thousands of user names. In this report to Congress, AT & T claimed that law-enforcement demands for cell phone information tripled between 2007 and 2011, when AT & T responded to nearly seven hundred requests a day. Because it was unclear in many jurisdictions whether or not law enforcement needed a warrant or court order to receive this personal data, the phone carriers asked Congress to set clearer standards for the police's right to receive GPS or other location information from citizens.

In June 2013, a scandal erupted in the United States when federal contractor Edward Snowden released the text of a court order allowing the FBI to download and record all call detail records created by Verizon for mobile-phone communications within the United States and between the United States and abroad. The data the FBI could capture included the phone numbers involved in the call, calling card numbers, and time and duration of the call. The data collection was allowed for three months, and it addressed not only people suspected of a crime but also all calls made during the period. The order contained no limit on how long the FBI could keep this information or what it could do with the data. Many people were surprised at the sweeping collection of mobile information and the many ways that the FBI could use this data to impinge on the privacy of any Verizon customer.

The US Supreme Court decided a case in January 2012 in which it required law enforcement to hold a warrant before placing a surveillance tracking device on a suspect's car and tracking his location every ten seconds for nearly a month.[22] The majority in this case found that the act of placing the tracking device on a car trespassed on the property rights of the car owner, and therefore required a warrant. This ruling is narrowly limited to circumstances in which the police place a tracking device on a suspect's property. However, the remaining four members of the court, with agreement on some positions by Justice Sotomayor, found that the cumulative act of monitoring movements electronically for several weeks was beyond what people would expect, and therefore it would have demanded a warrant simply based on the extent of the surveillance.

Since all members of the court felt that a warrant was needed for the surveillance of the suspect, how does their difference in reasons matter?

Because the majority's opinion relies on the concept of physical trespass by police on the property of the suspect, it does not help US courts faced with a question of whether law enforcement needs a warrant to pull smartphone location records based GPS or cell-tower triangulation. When police pull cell records, they are never trespassing on the suspect's property, only examining data, either current or historical, already being tracked by a suspect's telephone. In contrast, if the concurring opinion were law, it would give direction in these cases, and would likely mean that police would need a warrant to track a suspect over a long period of time using the tracking software included in mobile devices.

For now, lower US courts are left to wonder whether a warrant is necessary in tracking suspects through their phone records. No legislation or high court decision clarifies this point in the United States, so depending on where you live in the United States, the police may be able to track your movements by following your phone, even without probable cause to believe that you committed a crime.

PROTECTING DATA ON YOUR MOBILE DEVICE

Now that you understand what data is being captured by your mobile devices and who might want that information, you can take steps to control access and protect your privacy.

Protecting Your Data While Traveling

When you travel to countries such as China and Russia that are known to hack travelers' devices, take special precautions. Venerable computer publication *Infoworld* recommends that people visiting China leave their mobile computers at home, take only a loaner computer and/or a disposable phone, and have your work email forwarded to an outside email account that you can check periodically.[23]

Of course, you could go completely tech-naked, with no computing device at all, which, like abstinence, is the only way to positively avoid certain results. However, if you have to take your device overseas to one of the dangerous countries, do not let the device leave your presence. Sleep with it under the pillow and carry it with you everywhere. Also, turn it on only when needed, and do not allow Wi-Fi or Bluetooth connections to reach your phone.

Protecting Your Data at Home

Even when safe at home, you can take steps to protect the data on your mobile smartphone or tablet. First, take advantage of the protections provided by the phone itself. This is one place where security should outweigh convenience. Set a hardware encryption password, so that you not only slide your phone to open it, but you must enter a personal identification number or pattern as well. Android phones allow a secret gesture that you draw with your finger to unlock the screen.

You can also encrypt your data within the phone. Newer iPhones have encryption included in both the software and the hardware, making it very difficult for a stranger to crack. Certain Android phones such as the Samsung Galaxy S III also offer a password lock that encrypts and decrypts data on the phone. If the operating system does not offer this feature, you can find apps that will do it for you, such as Good Technology for either of the largest platforms, or SecureMemo for Android.

You can also find apps that will help you locate lost phones, so that if the device is turned on, you can ping the device and show its location on a map. Apple offers a free tool called Find My iPhone, and it searches for your phone from your iCloud account. An analogous app for Android is called Where's My Droid.

WEARABLE DEVICES THAT CAN TRACK AND CAPTURE YOUR INFORMATION

While the main discussion of this mobility chapter has been smartphones and tablets, certain wearable devices can track you as well. For example, Google Glass is a computer gadget mounted on a frame that you wear like glasses. It provides an Internet overlay onto your vision of the real world that will undoubtedly include sensors that can track your location and capture information from your web-surfing habits to the applications you use most often. Other wearable computers, including wristwatch computers that Apple is developing,[24] will collect data about their wearers and have similar tracking capabilities as current smartphones.

In the spring of 2013, Disney introduced a vacation management system called MyMagic+ that includes computerized wristbands that keep track of your activities at Disney theme parks, providing your family with a more customized park experience. Imagine approaching a Sleeping Beauty character that automatically knows your daughter's name and knows that her birthday is coming soon. The MagicBand functions as a room key, park ticket, FastPass for parking, and credit card at the parks. It allows other customization as well, such as the option to receive special offers, preselect three FastPasses before you leave home to reduce waiting time on rides, or choose whether to share your children's names with park employees. In exchange for greater convenience and a personalized park experience for the whole family, you are allowing the park to track all your transactions and rides.

Great Wolf Resorts, owner of eleven water parks in North America, has been using radio-frequency wristbands since 2006 to track visitors to its parks. Great Wolf Resorts uses the wristband system to pay for food and beverages on account. The bands have been well received because they free guests from the need to carry money or keys on the waterslides. But the bands also allow the resort company to track you and your family through the park for the full length of your visit and tie all activities and purchases to your name.

In the mobility space, privacy and personal information is traded for convenience, and the theme park wristband system is one of the best examples of this trade-off. Choosing more convenience allows the companies owning the park to mine a universe of data about you, your family, and the transactions you conduct.