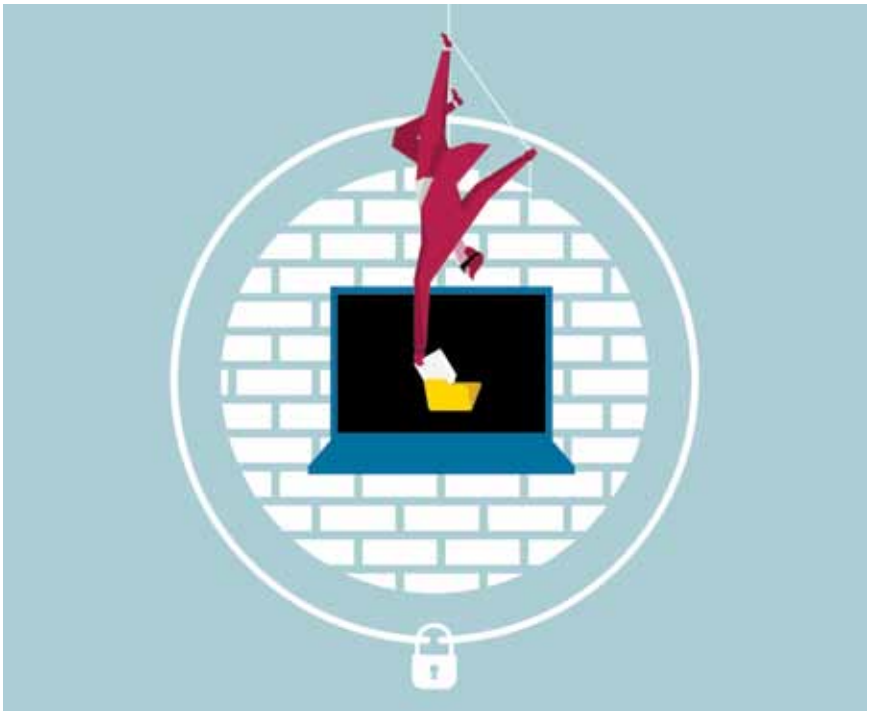
Technological Advancements Coexisting with Tech Stagnation

By Judge Herbert B. Dixon Jr.



In the last issue of *The Judges' Journal*, I wrote an introduction entitled "Technology Changes Coming Faster and Faster," which prompted me to review recent advancements involving subjects of several of my previous articles. It is no surprise that some of my past articles are outdated because of technological advancements. However, there is one subject, the security of digital data, where I remain gravely concerned because of continuing vulnerabilities. Following my review, I selected the three articles below, outlined the significant points in each article, and discussed technological developments since this *Journal* published that article.

Scientific Fact or Junk Science? Tracking a Cell Phone Without GPS

The Judges' Journal, Winter 2014

This technology article, written one year ago, is now nearly obsolete. In it, I discussed an ongoing dispute among experts whether the approximate location and movement of a cell phone without Global Positioning System (GPS) could be determined and tracked. Well, the technology is so advanced now that your cell phone (oops, I intended to say smartphone) should not only be able to report your building location, but also indicate whether you are on the first, fifteenth, or twenty-second floor, or higher.[1]

Tracking a Cell Phone to a Building and the Floor It Is On

The Federal Communications Commission is considering new rules that would require wireless carriers to build more precise location systems capable of finding callers anywhere, even in a multistory building, and may have adopted such rules by the time you receive this copy of the *Journal*. The background giving rise to the proposed new rules is that more than 100 million smartphones contain barometric pressure sensors that are capable of making air pressure readings to estimate, within a few feet, the altitude of the device. Some readers may already have experienced evidence of this altitude-sensing capability from a health app on their smartphone that analyzes changes in air pressure to estimate the number of floors of stairs they climbed each day. The adventurous among you also may have discovered this feature while using a smartphone app to keep track of your altitude while mountain climbing, hang gliding, or sky diving. The scientific principle on which this capability works is straightforward. Air molecules concentrate more densely at low altitudes than at high altitudes. These variations in molecule concentration at various heights are used to calculate or estimate the device's altitude.

In essence, the GPS capability is providing your x and y coordinates and the barometric-pressure sensor is providing the z coordinate, a three-dimensional graph. The possible uses of these new capabilities include, for example:

1. A multi-floor department store sending a special coupon to your smartphone as you pass through the store's shoe section;
2. Employers tracking the floor-by-floor and room-by-room movement of employees who are handling valuables; or
3. Law enforcement pinpointing the location of a victim or suspect.

Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, a member of the ABA Board of Governors, and a former chair of the National Conference of State Trial Judges. He sits on the Superior Court of the District of Columbia and can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter@Jhbdixon.

Of course, these capabilities raise privacy concerns: The government, private businesses, and hackers could use these three-dimensional location data to track people for inappropriate purposes.

Giving a Wireless iPad Presentation: Where Perfect Is the Enemy of Good

The Judges' Journal, Winter 2012

This article, published three years ago, discussed the thrill of walking around with an iPad making a wireless presentation on a room video display (projector or large monitor) using an iPad, an Apple TV, a wireless network, and a digital HDMI[2] cable to connect the Apple TV device to the room video display.

The article noted the requirement for a powered HDMI to VGA[3] adapter when connecting the Apple TV to the monitors to display the presentation for the audience, unless the input connection was already a digital HDMI cable. I complained about the need for this powered converter. The article also discussed the need for wireless Internet access or a wireless Internet router, and revealed the secret (to some) that the router did not require an Internet connection. As it turns out, the router signal (even though not connected to the Internet) can be the medium for the Apple TV to communicate wirelessly with the iPad. From this wireless connection, the Apple TV sends the iPad's video and audio to the output display monitors.

A Wireless iPad Presentation No Longer Requires a Powered HDMI to VGA Converter

One nuisance requirement discussed in the article, a powered (i.e., plugged into an electrical outlet) HDMI to VGA converter to convert the Apple TV's HDMI output to the older VGA input still found in many courtrooms and conference rooms, has been alleviated! Within a few months of that article's publication, companies began producing an HDMI to VGA converter that operates without external power. This product was tremendously helpful because it eliminated one of the wired connections needed to make a wireless iPad presentation. Included among these new converters were the Kanex ATV Pro HDMI to VGA Adapter and the Belkin HDMI to VGA Adapter.

A Wireless iPad Presentation No Longer Requires Wireless Internet Access or a Wireless Internet Router (provided you have the correct model Apple TV)

A second nuisance requirement discussed in the article has been eliminated (for some): the need for either wireless Internet access or a wireless Internet router. About a year after publication of this article, Apple produced a new model of its 3rd generation Apple TV (which Apple should have called Apple TV 4th generation, but I digress). The new model of Apple TV3 introduced a feature called "peer-to-peer AirPlay." The good news is that this new feature enabled the iPad to transmit video and audio wirelessly to the Apple TV without any wireless Internet access or wireless Internet router. The bad news is that peer-to-peer AirPlay is not available on the original Apple TV3 or any previous model of the Apple TV device. What a bummer! I still need wireless Internet or a wireless Internet router to give my wireless iPad presentations because I only have an Apple TV1 and the first Apple TV3 devices, neither of which has peer-to-peer AirPlay—another example of "Technology Changes Coming Faster and Faster."

Cybersecurity . . . How Important Is It?

The Judges' Journal, Fall 2012

This article, published 18 months ago, discussed malicious computer hacking and predicted more to come if the threat were not taken seriously. The article highlighted:

- General Keith Alexander, head of both the National Security Agency and the U.S. Cyber Command, addressing the annual meeting of the oldest and largest gathering of computer hackers; speaking about a 17-fold increase in cyberattacks; and estimating that, on a scale of 1 to 10, U.S. preparedness for a large-scale cyberattack "was around a 3";
- The president of the United States taking the unprecedented action of writing an op-ed article in *The Wall Street Journal* to urge passage of the Cybersecurity Act of 2012 to prevent large-scale cyberattacks by hackers on the nation's critical infrastructure (the Act, by the way, was not passed);
- The ABA president adopting and pursuing cybersecurity as a priority initiative for the ABA; and
- A prominent and highly respected technology writer being the victim of malicious hacking that resulted in all data being wiped from his iPhone, iPad, and MacBook; access to his iCloud and Gmail accounts being blocked; hijacking of his Twitter account; and the loss of many important documents, including family photographs.

After everything discussed in that article, I hoped I had gotten the world's attention and convinced everyone to shore up their cyber defenses, but I was brought back to reality by two events that occurred within the last six months.

The Biggest Impediment to Maximizing Cyber Defenses Is People

First, JP Morgan Chase was the victim of a massive attack in which the hackers obtained vast access to large volumes of checking, savings, and other bank account data. The president of the United States, General Alexander, and the ABA president had warned about this type of attack. More importantly, subsequent investigations suggested that the theft of valuable records would have been minimized had a routine security fix, two-factor authentication (which requires a second one-time password to gain access to a protected system), been installed on an overlooked server in JP Morgan's network. JP Morgan's security team had apparently neglected to upgrade one of its network servers with the dual-password scheme, which left the bank vulnerable to intrusion.[4]

The second event that occurred recently was the hacking into the computer systems at Sony Pictures Entertainment. The results were devastating. Sony's operations were

paralyzed for several days, including the loss of basic e-mail; employee information was revealed, including salaries of top employees; nasty and insensitive e-mails were revealed; movies that had not been released were posted on file-sharing websites; and scripts of movies not yet made were stolen. One estimate of Sony's losses from this one incident is up to $75 million.

Some information technology security experts were not surprised by the Sony hacking because all networks are vulnerable to a sufficiently skilled, funded, and motivated hacker. However, they were surprised by the extent of access that the hackers gained. Those experts say that cybersecurity must be a combination of prevention, detection, and response—prevention to make targeted attacks harder; detection to spot the attackers; and response to minimize the damage, restore security, and manage the fallout.[5]

As attributed to the French writer Jean-Baptiste Alphonse Karr, "the more things change the more they stay the same." Change is a part of technological advancement, which is why the cell phone/smartphone advancement is not surprising and the increased capabilities of computers, tablets, and Apple TV devices also should have been expected. However, the failure to advance information security by some who should know better is both surprising and alarming.

We need more than the locked file cabinets and armed guards that protect physical valuables. We need robust protection systems and protocols to protect our digital valuables, including digital files at law offices, courts, private industry, and government entities, and we need to adhere to these protocols.

In addition, do not forget your individual role in strengthening our cyber defenses with strong passwords. Take a look at the technology article in the Spring 2014 issue of the *Journal*: "Worst Passwords of 2013." As certain as anything else in life, the list of the worst passwords of 2014 will also include "password" & "123456" at the top of the list, the same as in 2013 and previous years.

Two years from now, I hope I will not be writing about even more devastation from hacking that could have been minimized simply by people being more conscious of cybersecurity. ■

Endnotes

1. Craig Timberg, Cellphone Tracking: Find an Address? Easy. But New Devices Can Calculate Your Altitude, Wash. Post (Nov. 19, 2014), http://www.washingtonpost.com/business/technology/cellphone-tracking-find-an-address-easy-but-new-devices-can-calculate-your-altitude/2014/11/19/a47a85b2-6a85-11e4-b053-65cea7903f2e_story.html?tid=HP_more?tid=HP_more.

2. High Definition Multimedia Interface.

3. Video Graphics Array.

4. Matthew Goldstein, Nicole Perlroth & Michael Corkery, Neglected Server Provided Entry for JPMorgan Hackers, N.Y. Times (Dec. 22, 2014), http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified.

5. Bruce Schneier, Sony Made It Easy, but Any of Us Could Get Hacked, Wall St. J. (Dec. 19, 2014), http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.