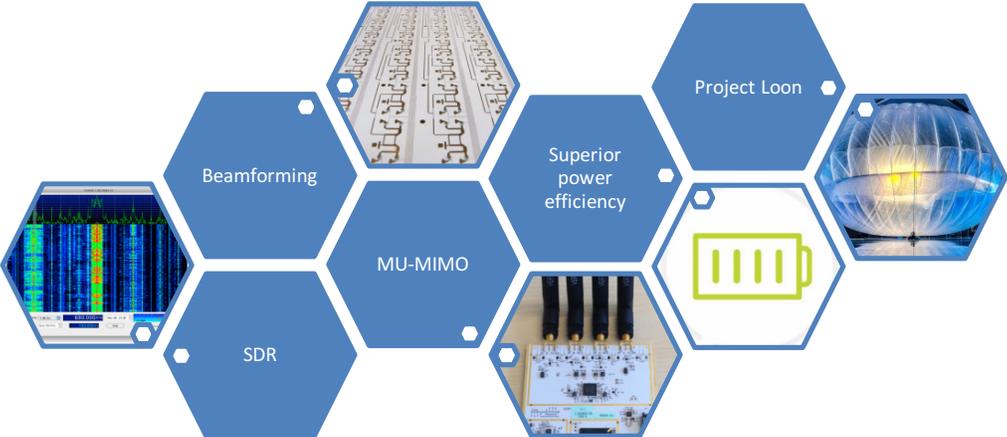


# THE 2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

## WIRELESS DEVICES IN THE WORKPLACE



## Research Team Members

<u>NAME</u>	<u>ORGANIZATION / AGENCY</u>
<u>Matthew G.</u>	<u>ODNI</u>
<u>Barbara Tl.</u>	<u>FBI</u>
<u>Douglas Blough</u>	<u>Boeing</u>
<u>Hany Wassef</u>	<u>Meritor</u>
<u>Jack Voth</u>	<u>Algenol Biotech, LLC</u>
<u>John N.</u>	<u>DoD</u>
<u>Yev F.</u>	<u>DHS</u>
<u>Patrick Mullins</u>	

## ACKNOWLEDGEMENTS

As part of the Public-Private Analytic Exchange Program, a working group, comprised of public and private sector analysts, examined issues and concerns surrounding the use of wireless devices in the workplace.” The Wireless Devices in the Workplace (WDW) working group (the "Group") focused primarily on beamforming, Internet of Things (IoT), Software Defined Radios (SDR), and wireless security. The Group received additional research support from:

- SparkFun Electronics
- Panasonic CityNOW/Pena Station NEXT
- NIST Boulder
- NIST Gaithersburg
- National Instruments formerly Ettus Research
- Bastille

## INTRODUCTION

Gone are the days of your standard Wi-Fi router operating in the 2.4 GHz range with transfer speeds up to 54Mbps (802.11b), the 5.8 GHz range with transfer speeds up to 11Mbps (802.11a) or 3G cellular technology operating up to speeds of ~2Mbps (Kumar, Liu, Sengupta, & Divya, 2010). Users today have access to much faster communication in the form of 802.11ac Wi-Fi, 4G, GSM, LTE, Bluetooth, 5G (in 2016), among others. All the speed and functionality of our technology has dramatically increased, while other aspects of our technological advancement have lagged behind.

New enabling technologies such as 5G communications, Software Defined Radios (SDR), Multiple-Input Multiple-Output (MIMO), or Google’s Project Loon all promise a more connected world.

Wireless security has been and continues to be a challenge. Bring Your Own Device (BYOD) has created new challenges for all security departments across all sectors both public and private. The growing Internet of Things (IoT) market continues to expand the attack vector for networks, including additional connected end points and limiting the ability of the user to update and patch those end points.

As with all technology, the promise of speed, versatility, and functionality come with the risk of breach. These breaches range from the more benign, such as a breakdown in communication, to the more nefarious, such as the public release of private information. How is the end-user to balance the costs associated with first adopter technologies, with the necessities of protecting Personally Identifiable Information (PII)? How is the end-user to know which technology is best for them? As a service to the public, the Group has created a rating system designed to

quickly and clearly identify to the consumer the level of technology security for wireless devices. The rating system is called the “**Consumer Confidence Rating**”.



This rating system is a five (5) star rating system. A one (1) star rating would be very basic and insecure. A five (5) star rating would have many configurable security features. These confidence ratings will allow end-users to choose what confidence rating is right for them, much like the Insurance Institute for Highway Safety (IIHS). The IIHS uses Good, Acceptable, Marginal, Poor. As a consumer I can balance cost and safety, choosing the automobile which is right for me. The Customer Confidence Rating will allow end-users to make more informed decisions about the devices they purchase and incorporate into their networks.

## The Wireless Environment

The current wireless environment is growing exponentially. Mobile data traffic is expected to grow eight-fold in the next five years thanks to emerging technologies like mobile video, video-over-LTE (ViLTE), voice-over-WiFi (VoWiFi), voice-over-LTE (VoLTE). Smartphones alone will account for 81 percent of global mobile traffic by 2020 and will reach 367 exabytes, up from 44 exabytes in 2015. In 2015 the 4G LTE connections reached 1 billion subscribers worldwide. The number of unique subscribers is expected to reach 5.6 billion by the end of 2020 (Cellular News, 2016).

Wearable devices, like smartwatches, will grow six-fold by 2020, with more than 600 million wearables in use, up from 97 million in 2015 (Computerworld - Hamblen, Matt., 2016).

Google has plans to cover the globe with balloons to provide 4G-like speeds to everyone, including underdeveloped countries with Project Loon (Kelion, Leo - BBC., 2015). Google, under its Project Loon, is using big balloons floating at a height of 20 km (12.4 miles) above the earth surface for transmission of internet services (Google, 2016). Google has approached the Indian government to set up the Loon project that has the potential to replace mobile towers as it can directly transmit signal on 4G mobile phones (Press Trust of India, 2016).

US firm Iridium Communications Inc said its Satellite Time and Location (STL) system was ready for use as an alternative or companion to the US Air Force's Global Positioning System (GPS) satellites (Reuters, 2016).

Narrow Band Internet of Things (NB-IoT), as the name suggest will be implemented in the IoT market. Narrowband IoT (NB-IoT) is a standards-based Low Power Wide Area technology developed to enable a wide range of new IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Battery life of more than 10 years can be supported for a wide range of use cases (GSMA, 2016).

Beamforming Devices that support beamforming focus their signals toward each client, concentrating the data transmission so that more data reaches the targeted device instead of radiating out into the atmosphere. Beamforming can help improve wireless bandwidth utilization, and it can increase a wireless network's range. This, in turn, can improve video streaming, voice quality, and other bandwidth- and latency-sensitive transmissions (Geier, 2013).

The current wireless space is complex and multi-faceted. It is in our everyday lives, our professional lives and our personal lives. It will soon be, and in some cases already is, embedded in our appliances both in our homes and our workplaces. These devices will make our lives more convenient but at the same time make our lives less secure.

## New Enabling Technologies

The rapid market adoption of the smart phone has been a leading driver in creating the necessary foundational pieces that enable the Internet of Things. Smartphone manufacturers have invested massive amounts of money, and the technology that has driven to make phones smaller, faster, and longer lasting directly enable our interconnected world.

What's coming next? Advances in power sources and power efficiency as well as wireless networking will drive the next generation of connected devices. Looking out at the horizon, major players launching "moonshot" programs will profoundly change the future.

### Power

Modern industrial design pushes consumer devices to become smaller and lighter, with consumers demanding no loss – or even increases – in device battery longevity. These competing forces are leading to research to make batteries more power dense to achieve both goals.

A leading contender in this race to create more power dense batteries is Lithium-Air batteries, or "Li-air". Worldwide, research is underway on this promising technology, which has the potential to increase the power density of batteries by a factor of 5x to 8x as compared to current Lithium Polymer (LiPo) batteries, the current mainstay of smartphone power sources (Lu & all, 2016).

The advances that Li-air batteries can enable include further miniaturization of devices, integration of devices in embedded systems, and devices capable of running for months or years on a single charge. All of this enables the proliferation of "smart" devices as a part of the Internet of Things.

Researchers are also working on the other side of the power equation, by reducing the power usage of modern processors. Traditionally, computing has been known to follow Moore's Law – roughly stating that the overall processing power for computers will double every two years. Moore's Law has stood the test of time, and computing power has generally followed this progression for the last 50 years. However, there are signs that outright computer processing power is beginning to stagnate, as gains based on further miniaturization of transistors begin reaching the atomic scale and show diminishing returns.

Against that backdrop emerged Koomey's Law – which roughly states that for a fixed computing load, the amount of power required will fall by a factor of two every 18 months. Koomey's research has shown this trend to be historically accurate and stable since the 1950s (Koomey, 2010).

Koomey's Law can be seen in action by examining the increases in battery life realized in the most recent generations of smartphones. For example, the iPhone 6s has a battery with 6% less

capacity, and features similar rated battery life despite a 70% improvement in processing power and additional sensors (Mitra, 2016).

Increases in device longevity and computing power will enable new generations of smart sensors and devices to be deployed, generating a vast set of high quality data streams for larger systems to leverage.

## **Wireless Networks**

How will these more powerful and longer-lasting devices communicate? Embedded devices with low-bandwidth requirements will see connectivity coming from low power wide area networks (LPWANs) such as LoRaWAN and SIGFOX.

SIGFOX is a French company focusing on wireless connectivity for low power devices – primarily the sensors that put the “smart” in “smart technologies”. LoRaWAN is a network specification backed by the LoRa Alliance, aimed squarely at the same market. Both technologies promise low power use and long range – enabled by aggressive duty cycle management and low data rates. These technologies, and perhaps emerging similar technologies will be the mainstay for smart sensors and the Internet of Things. However, their low data rates make them ill-suited for modern end user devices (Knight, 2106).

Bandwidth hungry end user devices – smartphones, tablets, in-vehicle data hotspots – will require next generation mobile networks, 5G networks. These new mobile networks will be defined by millimeter wave bands (20-60 GHz), multiple-input and multiple-output (MIMO) antenna systems, and beamforming techniques.

Millimeter wave band systems for mobile devices will operate in the 20-60 GHz range. Networks operating in these ranges will be characterized by line-of-sight requirements, atmospheric attenuation, and interference from buildings and foliage. These limitations can be mitigated by the use of MIMO antennas and beamforming, and do provide for some benefits in terms of allowing greater spectrum utilization through frequency reuse based on the limited signal propagation. Expected data rates for 5G millimeter band systems greatly exceed 1 Gigabit per second (Gbps) (Rappaport, et al., 2013).

MIMO antenna systems utilize multiple transmit and receive antennas to exploit multipath propagation to achieve increased capacity. Without MIMO techniques, the multipathing caused by signals reflecting off of building in an urban environment, for example, would lead to signal loss. Instead, digital signal processing is used to take advantage of the multipath signals to transmit multiple data streams in parallel on the same channel. This is a key enabling component of 5G mobile networks (Sampath, Talwar, Tellado, & Erceg, 2002).

A final important component of 5G networking is beamforming. To take advantage of the directional nature and minimal propagation of millimeter wave band systems, base stations will

feature phased array antenna systems. These systems will enable the base stations to “steer” bandwidth directly to end user devices, allowing for the increased spectrum utilization that millimeter wave bands afford by directing very wide bandwidth, but very small directionally shaped beams to each device with minimal interference for other devices connected to the base station (Van Veen & Buckley, 1988).

The expected jumps in bandwidth that 5G networking is projected to deliver will enable new classes of connected applications – bandwidth will no longer be a limiting factor for mobile devices. This will enable mobile devices to connect with and draw data from a large number of high quality data sources simultaneously to enrich the use experience.

### **“Moonshots”**

Just as the Apollo space program provided a huge boost to the scientific and engineering fields, several private companies are launching large scope projects to bolster internal technical teams, foster innovation, and create a cadre of employees that can think big and execute on a global scale. SpaceX has plans to launch missions to Mars starting in 2018, culminating in manned missions in 2022 (Foust, 2016).

Back here on earth, Google and Facebook are both launching efforts to deliver the internet to every person on the planet. Google’s approach – called Project Loon – features high altitude balloons; Facebook’s Project Aquila features solar powered, high-endurance, unmanned fixed wing aircraft. Both will provide wireless internet connections to the remaining populations without regular, affordable connectivity.

Google’s Project Loon uses high altitude balloons, inspired by weather balloons, to create an aerial wireless network with bandwidth similar to 4G-LTE networks. In fact, as Project Loon has evolved, it has gone from a proprietary platform to a means to extend the wireless footprint for telecom providers wishing to reach rural and remote users via LTE, with Google partnering with local service providers. Google has built the capability to launch and manage thousands of balloons – with full service expected to come online in the next 12-24 months. (Google 2016)

Facebook, too, is attempting to bring the internet to the estimated 5 billion people not currently connected. Project Aquila uses solar-powered, high-altitude, unmanned fixed wing aircraft. An early Aquila prototype flew on 28 June 2016. It is important to note that while Facebook has impressive plans for Aquila – including laser ground-to-air communications channels for multiple Gigabit bandwidth – they are at a much earlier stage than Google. The prototype that flew in June lacked solar panels and the communications gear required to connect users to the internet (Newton, 2016).

Loon and Aquila show what large companies with talented engineers can achieve. Google’s Project Loon is nearly ready to launch for full scale operations. When both projects are online, the entire planet will have internet access – even the most remote locations. These large scale

projects will ensure that wherever you are, you will be connected to the internet, and the internet of things will be connected to you.

## Wireless Security Challenge

Wireless communication devices are becoming ubiquitous in our everyday lives and provide increasing usability and functionality for the end user. With increased functionality and ease of use, there are also increased security risks resulting from a greater attack vector. The use of software defined radios and high gain antennas allow malicious actors to be relatively far from the target, but still interact with it wirelessly.

One example of an attack that impacts a relatively new convenience feature is relay attacks on Passive Keyless Entry and Start (PKES) systems that are utilized in many modern cars. The PKES system allows the car owner to open a car door when the key is within a few foot proximity area to the car and start the car when the key is inside the car. Researchers at ETH Zurich were able to create inexpensive relays that allowed the attacker to enter and start the car from a much larger distance than intended by the manufacturer. The attackers performed the evaluation on 10 car models from 8 manufacturers and their results showed that relaying the signal from the car to the key was “sufficient to perform the attack while the true distance between the key and car remains large (tested up to 50 meters, non-line-of-sight)” (Francillon, Danev, & Capkun, 2011)

The cyber security company Bastille, discovered a wireless attack involving wireless mice that use a USB dongle to communicate with the computer. This vulnerability impacts some wireless mice from well-known companies like HP, Lenovo, Amazon and Dell. A security researcher at Bastille explains that these manufacturers “haven't encrypted the mouse traffic, that makes it possible for the attacker to send unencrypted traffic to the dongle pretending to be a keyboard and have it result as keystrokes on your computer. This would be the same as if the attacker was sitting at your computer typing on the computer” (Gruber, 2016). This attack can be performed with under \$20 of readily available hardware plugged into the attacker's computer and allows the attacker to send 1000 words a minute to the target machine, at that rate it may only take a few seconds to take over a computer and gain network access. This attack can work from as far as 180 meters, and none of the security on the target machine or network would identify these attacks because it is coming through an approved dongle plugged in so the user can work without a wire connecting their mouse to the computer.

Internet of Things (IoT) devices are becoming increasingly common and each device increases the attack vector for malicious actors. Researchers at Princeton found vulnerabilities in many IoT devices currently on the market, many of them leaking information about the user. The researchers warn that information, such as if a user is home and their activities are all sent to the cloud. Other devices such as the PixStar Digital Photoframe were found to send information unencrypted, making it available to anyone that might be listening (Davis, 2016).

The rapidly expanding smartphone space and the concept of Bring Your Own Device (BYOD) have created new vulnerabilities in both the corporate and home environments. Ten years ago, it was standard practice for companies and other large organizations to issue BlackBerry phones with BlackBerry Enterprise Server (BES) software. This software provided employees with access to company networks that offered reliability, security and manageability. By 2007, iPhones and Android Smartphones became available and employees began to carry two devices; one for personal use and one for work. Companies such as Good Technology have enabled IT departments to embrace the BYOD trend while maintaining security and manageability. Corporations began to address the BYOD trend by enabling personal devices to connect to corporate applications. Research analysts at Gartner, a leading information technology research and advisory company, pointed out those companies would have to recognize that the right of users to employ the capabilities of their personal phone conflicts with enterprise mobile security policies, as well as, increases the risk of data leakages and becoming exploitable vulnerabilities. (Taylor, 2013)

According to Cisco Labs' 2012 analysis of educational campus networks, in a BYOD environment, the most effective approach to mobile security is enforcing security policy in the network. Network-based enforcement makes the device and connection method, whether wired, wireless or VPN, irrelevant. They recommend that in any BYOD environment, the network needs the intelligence to:

- Know the identity of the person and the device accessing the network
- Automatically detect and mitigate web-based threats that may lead to security breaches
- Maintain private information so that it is not compromised
- Creating a unified policy definition on all networks

Cisco Labs also discusses that many of today's threats spread when people visit websites. An environment with a BYOD policy needs a solution for URL filtering, malicious code detection and filtering and application controls for popular web-based applications. As a result, Cisco promotes that their products provide solutions for enforcing wireless security policies. Such capabilities include the ability to identify user authentication, encryption and access control.

It is also capable of detecting and containing unauthorized wireless access points, monitoring and detecting wireless network anomalies and radio frequency attacks and automates wireless security vulnerability assessment. (Cisco, 2012) However, when developing wireless security policies, at least one challenge could arise. Allowing a policy to be created by a security team that operates in isolation alienates the rest of the organization. Separately, security policies are often written by people who have security expertise but not policy expertise. It's one thing to know how a security environment should be constructed, but translating this into a written set of enforceable rules is a discrete skill. (Rob McMillan, 2014)

McAfee has released a report on mobile security, claiming the rise in popularity of the smartphone has made it an attractive proposition for cyber criminals. According to the report, 19 per cent of users store credit card details on their phone. Alarmingly, 23 per cent store passwords and pin codes as well, without any form of remote locking or a password lock on a device to keep the thief away from your details. The report even suggests that individuals utilize internet banking for when they are at home or on a secure network. (Griffin, 2011) However, as cities like NYC look to expand broadband throughout the city, will consumers be more vulnerable at a larger scale as a result of the expansion? The ConnectHome program will bring affordable, residential broadband access within reach of more New York City Housing Authority households, complementing the wireless networks the administration is building in Queensbridge, Red Hook and Mott Haven. Both initiatives are part of the City's broader strategy for getting to universal affordable broadband by 2025. (NYC Press Release Office, 2015) Two questions arise: 1. Will consumers in such large housing complexes have the knowledge about applying security protocols with their devices in their home and 2. Will cybercriminals target the complexes broadband to manipulate the network traffic or perform intrusion on consumers' devices?

According to broadband guides, one of the biggest security issues consumers will face is home wireless broadband. If you do not set up a secure wireless network, you may be exposed to people hacking into your wireless network, also known as a WLAN. (USSwitch.com, n.d.) Hackers would be able to steal details from personal computers. These hackers, otherwise known as "war drivers", pursue wireless network security. This specific guide suggests setting up a home wireless network with proper security, by following your broadband provider's instructions for setting up your wireless network. It also recalls that WEP security is no longer very secure and can be broken very quickly, recommending the use of WPA2 instead.

Deb Shinder, a IT consultant and trainer, identifies that if an individual has the option to connect to a 3G/4G device via either wifi or USB tethering, the direct connection to the device is recommended because you eliminate the possibility of data transmitted between the device and the laptop being intercepted wirelessly. However, she emphasizes that it's important to realize that laptops and desktops connected to the internet via cellular transmissions need to be protected, as well. She also noted specific standard precautions to take: (Shinder, Security Issues when Connecting Computers to Cellular Networks, 2011)

- ensuring that the 3G/4G device whether a USB modem, a MiFi device, a card or a smart phone have all available updates installed to address vulnerabilities in the firmware or software
- have a firewall installed and properly configured on the host device
- have anti-virus and antimalware software installed and turned on
- use strong password or multifactor authentication for accessing sites involving financial data or PII

- enable logging and alerting
- for the wi-fi part of the connection, enable WPA2 encryption
- On a mobile hotspot device such as the MiFi or Sprint's Overdrive, disable SSID broadcasting and disable the DHCP server
- When using a mobile hotspot device or the mobile hotspot function on your phone, which allows for multiple computers to use the 3G or 4G connection, monitor the hotspot software to be sure only devices you know about are connected
- If the device allows you to set a maximum number of users, set this to 1 if you are going to be the only one connecting to the device
- Change the default administrative passwords on your 3G/4G devices
- If your 3G/4G device supports MAC filtering, enable it and create a white list of the physical addresses of devices (such as your laptop) that you want to be able to use the 3G/4G network, and block all others

It should be noted, in many of Shinder's articles, she re-iterates that BYOD offers advantages for both the individual users who bring their own devices to work and for the companies that implement BYOD programs – if those programs are implemented correctly. (Shinder, The Android Invasion: BYOD Security Implications and Solutions, 2013)

## Wireless Security Proposal

We propose a Monroney Sticker like system used in the automobile industry for crash ratings to assign a security rating from an independent governmental organization similar to the National Highway Traffic Safety Administration.

**VEHICLE DESCRIPTION**  
**FORD FUSION**  
 DR 150430  
 EXTERIOR: VOLTAGE IMPACT BLUE  
 INTERIOR: CHARCOAL BLACK CLOTH SEATS

**FUEL ECONOMY AND ENVIRONMENT**  
 EPA DOT Fuel Economy and Environment Gasoline Vehicle  
 Fuel Economy: 28 MPG (combined city/hwy), 23 city, 36 highway  
 You Save \$2,100 in fuel costs over 5 years compared to the average new vehicle.  
 Annual Fuel Cost: \$1,900  
 Fuel Economy & Greenhouse Gas Rating: 7  
 Smog Rating: 10

**GOVERNMENT 5-STAR SAFETY RATINGS**  
 Overall Vehicle Score: 7 (To Be Rated)  
 Frontal Crash: Driver (To Be Rated), Passenger (To Be Rated)  
 Side Crash: Front seat (To Be Rated), Rear seat (To Be Rated)  
 Rollover: Not Rated

**DEALER INFORMATION**  
 Ford Motor Credit Company  
 Total MSRP: \$25,585.00

The purpose of the Customer Confidence Rating is to illustrate in a clear and concise manner what device is being evaluated, what the devices rating is, the justification for the rating, the organization responsible for assigning the rating, and where the consumer can find more information about the rating system and the device.

See attached example:

The rating system will be as follows:

- 5 Star**  
★★★★★

  - Can detect and prevent cyber-attacks (Botnet communication, Malware in data streams, drive by downloads...etc)
  - Can alert on different attacks (email, SMS, injection of HTML warning banners, etc.)
  - Has a mechanism to keep Attack Signatures up to date
  - Can block traffic based on Geolocation and IP reputation data
- 4 Star**  
★★★★

  - Device supports logging for extend period of time (30 days or more) to facilitate analysis in case of cyber security incidents
  - Logging level is adequate to understand at least the 3Ws metrics (who, when and what)
  - Log exporting and archiving features
- 3 Star**  
★★★

  - Access to management interface can only be achieved through secure protocols (HTTPS, SSH v3, ..etc)
  - Access to management interface can be restricted to physical ports vs. wireless or through unsecured network ports. Good example is it use the Console port or any other detected interface.
  - Management accounts can handle brute force attacks (lockout, one time passwords.. etc)
- 2 Star**  
★★

  - Code has been signed by the vendor's certificate, Chain Block or PGP key
  - The device authenticates the source of the firmware update and checks the vendor's electronic signature before applying it.
  - Each device has its own unique management password that can't be driven from known parameters
- 1 Star**  
★

  - Code has been reviewed and found to be free of known bugs and vulnerabilities by qualified third party entities.
  - No hard coded accounts or passwords
  - Firmware/Low level code can be updated

## Conclusion

The technology that enables wireless communications continues to get increasingly faster with the development of enabling technologies, including 5G networks and the utilization of MIMO antennas, and low power wide area networks. The availability of wireless communication technology is also spreading, though projects such as Google's Project Loom and Facebook's Project Aquila. Additionally, the power storage of batteries keeps increasing while the power consumption of devices keeps decreasing, as shown by Koomey's law. The combination of more efficient devices, faster wireless networks, and increased wireless network availability is connecting more users to the web every day.

The growing number of connected devices in all sectors, public and private, and in both business and personal use is exponentially increasing the attack surface, which puts everyone at risk. Multiple researchers, as well as real-world malicious actors, have demonstrated the security challenges that arise from a more connected world, but the convenience that many of these devices bring out weight the risks associated with them.

The consumer may not understand all of the security concerns of wireless devices, but they know the conveniences that they provide. For this reason, the group believes The Customer Confidence Rating would be such a valuable tool for the consumer, allowing them to make a more informed decision based on a simple five-star rating system that is easy to understand and does not require an in-depth knowledge of wireless communication technology and security concerns. Consumers could depend on a trusted system and device manufacturers would have an increased interest to build better security into wireless devices. Over time, consumers may come to use the Customer Confidence Rating when making purchasing decisions, just as car shoppers use the IIHS Crashworthiness ratings when evaluating competitive models.

The development of wireless communication technology and the complexity of wireless devices will only continue to increase. With these increases, the consumer will have an increasing need for a system to quickly and clearly identify the level of technology security for wireless devices.

## References

- Cellular News. (2016, March 2). *4G Connections Hit 1 Billion as Mobile Broadband Momentum Extends*. Retrieved from [www.cellular-news.com](http://www.cellular-news.com/story/Reports/68597.php): <http://www.cellular-news.com/story/Reports/68597.php>
- Cisco. (2012). *BYOD Security Challenges in Education*.
- Computerworld - Hamblen, Matt;. (2016, February 3). *Cisco sees eight-fold increase in mobile data by 2020*. Retrieved from [Computerworld.com](http://www.computerworld.com): <http://www.computerworld.com/article/3028755/mobile-wireless/cisco-sees-eight-fold-increase-in-mobile-data-by-2020.html>
- Davis, J. S. (2016, January 21). *Nest, other IoT devices, sent user info in the clear*. Retrieved from SC Magazine: <http://www.scmagazine.com/nest-other-iot-devices-sent-user-info-in-the-clear/article/466616/>
- Foust, J. (2016, June 13). *Musk gives details on SpaceX Mars plans*. Retrieved from SpaceNews: <http://spacenews.com/musk-gives-details-on-spacex-mars-plans/>
- Francillon, A., Danev, B., & Capkun, S. (2011, February). *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*. Retrieved from Syssec: <http://www.syssec.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/spot/332.pdf>
- Geier, E. (2013, Nov 8). *All about beamforming, the faster Wi-Fi you didn't know you needed*. Retrieved from [pcworld.com](http://www.pcworld.com): <http://www.pcworld.com/article/2061907/all-about-beamforming-the-faster-wi-fi-you-didnt-know-you-needed.html>
- Google. (2016). *Project Loon*. Retrieved from [Google.com](https://www.google.com/loon/): <https://www.google.com/loon/>
- Griffin, B. (2011, May 25). *McAfee: Attacks against mobile devices will escalate in 2011*. Retrieved July 21, 2016, from [Knowyourmobile.com](http://www.knowyourmobile.com): <http://www.citationmachine.net/apa/cite-a-website/search?utf8=%E2%9C%93&q=http%3A%2F%2Fwww.knowyourmobile.com%2Fproducts%2F13424%2Fmcafee-attacks-against-mobile-devices-will-escalate-2011&commit=Search+Websites>
- Gruber, B. (2016, March 23). *Wireless mice leave billions at risk of computer hack: cyber security firm*. Retrieved from [reuters](http://www.reuters.com): <http://www.reuters.com/article/us-usa-wireless-mouse-idUSKCN0WP21I>
- GSMA. (2016). *Narrow Band - Internet of Things (NB-IoT)*. Retrieved from GSMA: <http://www.gsma.com/connectedliving/narrow-band-internet-of-things-nb-iot/>
- Kelion, Leo - BBC;. (2015, October 28). *Google's Project Loon internet balloons to circle Earth*. Retrieved from [www.bbc.com](http://www.bbc.com): <http://www.bbc.com/news/technology-34660205>

- Knight, M. (2106, May 20). *Reversing Lora, Exploring Next-Generation Wireless*. Retrieved from Squarespace.com:  
<http://static1.squarespace.com/static/54cecce7e4b054df1848b5f9/t/57489e6e07eaa0105215dc6c/1464376943218/Reversing-Lora-Knight.pdf>
- Koomey, J. G. (2010, February 26). *Outperforming Moore's Law*. Retrieved from IEEE Spectrum:  
<http://spectrum.ieee.org/computing/hardware/outperforming-moores-law>
- Kumar, A., Liu, Y., Sengupta, J., & Divya. (2010, December). Evolution of Mobile Wireless Communication Networks: 1G to 4G. *IJect*, pp. 68-72.
- Lu, J., & all, e. (2016). A lithium–oxygen battery based on lithium superoxide. *Nature - International weekly journal of Science*, 377-382.
- Mitra, J. (2016, January 18). *iPhone 6S vs iPhone 6: the in-depth test*. Retrieved from Techradar:  
<http://www.techradar.com/us/news/phone-and-communications/mobile-phones/iphone-6s-vs-iphone-6-should-i-upgrade--1302313>
- Newton, C. (2016, June 28). *Facebook Takes Flight*. Retrieved from The verge:  
<http://www.theverge.com/a/mark-zuckerberg-future-of-facebook/aquila-drone-internet>
- NYC Press Release Office. (2015, July 15). *NYC.gov*. Retrieved 7 1, 2016, from New York City :  
<http://www1.nyc.gov/office-of-the-mayor/news/491-15/mayor-de-blasio-up-10-million-investment-free-broadband-service-five-nycha#/0>
- Press Trust of India. (2016, February 29). *Government wants Google to pick partner for 'internet balloon' project*. Retrieved from indiatimes.com: <http://timesofindia.indiatimes.com/tech/tech-news/Government-wants-Google-to-pick-partner-for-internet-balloon-project/articleshow/51186886.cms>
- Rappaport, T., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., . . . Gutierrez, F. (2013). Millimeter Wave Mobile Communications for 5G. *IEEE Access*, 335-349.
- Reuters. (2016, May 24). *Iridium launches timing, location service as GPS back-up*. Retrieved from Reuters/Technology: <http://www.reuters.com/article/us-iridium-gps-idUSKCN0YE1HZ>
- Rob McMillan, J. H. (2014, September 17). Five Golden Rules for Creating Effective Security Policy.
- Sampath, H., Talwar, S., Tellado, J., & Erceg, V. (2002). A fourth-generation MIMO-OFDM broadband wireless system: design, performance, and field trial results. *IEEE Communication*, 143-149.
- Shinder, D. (2011, July 20). *Security Issues when Connecting Computers to Cellular Networks*. Retrieved July 26, 2016, from Windowssecurity.com: [http://www.windowsecurity.com/articles-tutorials/misc\\_network\\_security/Security-Issues-when-Connecting-Computers-Cellular-Networks.html](http://www.windowsecurity.com/articles-tutorials/misc_network_security/Security-Issues-when-Connecting-Computers-Cellular-Networks.html)

Shinder, D. (2013, May 29). *The Android Invasion: BYOD Security Implications and Solutions*. Retrieved July 24, 2016, from Windowssecurity.com: [http://www.windowsecurity.com/articles-tutorials/Mobile\\_Device\\_Security/android-invasion-byod-security-implications-solutions.html](http://www.windowsecurity.com/articles-tutorials/Mobile_Device_Security/android-invasion-byod-security-implications-solutions.html)

Taylor, P. (2013, February 25). *Financial Times*. Retrieved July 22, 2016, from BYOD: Freedom of choice prompts security issues for IT chiefs: <https://next.ft.com/content/cc0a2782-7120-11e2-9b5c-00144feab49a>

USSwitch.com. (n.d.). *Broadband Security*. Retrieved July 22, 2016, from US Switch: [https://www.uswitch.com/broadband/guides/broadband\\_security/](https://www.uswitch.com/broadband/guides/broadband_security/)

Van Veen, B., & Buckley, K. (1988). Beamforming: a versatile approach to spatial filtering. *IEE ASSP Magazine*, 4-24.

**All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.**