“WHY” WAS THE SMARTPHONE INVENTED?

BY LARRY GOLDEN

THE GOVERNMENT WAS GIVEN NOTICE OF THREE ECONOMIC STIMULUS AND TERRORIST PREVENTION PACKAGES: “THE SAFERACK PROJECT”, “THE V-TECTION PROJECT”, AND THE ANTI-TERRORISM PRODUCT GROUPING (ATPG) PROJECT:

Six months after the DHS was established on Nov. 25, 2002, Petitioner receive a response letter on May 21, 2003 from the Honorable Senator Fritz Hollings: “I have contacted the Department of Justice and the Department of Homeland Security to try to be of assistance”; on June 3, 2003 from the Office of the Vice President, Dick Cheney: “[y]our correspondence has been forwarded to the Department of Homeland Security for review. You will hear back directly from the Department”; on October 1, 2003 from the Honorable Senator Fritz Hollings: “[t]hank

you for contacting me regarding your difficulty with receiving a response from the Department of Homeland Security"; on October 21, 2003 from the Honorable Senator Lindsey Graham: "I have contacted the Department of Homeland Security on your behalf. I have asked that they review your request and respond directly to you"; on June 20, 2005 from the Office of the President, George Bush: "[t]hank you for your letter regarding homeland security technology procurement. Please know I have forwarded it to the Department of Homeland Security for review and response". (STATUS REPORT: CD of Petitioner's Discovery Documents: CFC Case No. 13-307C; Dkt. No. 101; filed 02/17/2017). Also, copies of the letters can be found on my website: atpg-tech.com; click on *Larry Golden v. The United States*.

ADDITIONAL NOTICES GIVEN THE UNITED STATES

I. 2006: DoD/DARPA/SPO; BAA06-02; A.1.4 Defense against Chemical Biological Radiological Weapons. Abstract for Review to the Attention of Deputy Director Brian Pierce, Dr. Wayne Bryden, Mr. Thomas P. McCreery

II. 2006: HSARPA/SBIR; 1.1 DHS S&T TOPICS; SBIR/STTR TOPIC NUMBER: H-SB06.2-001; TITLE: SYSTEM FOR DESIGNING AND EVALUATING CHEMICAL OR BIOLOGICAL AGENT SENSOR NETWORKS. Abstract for Review to the Attention of: Mr. Mike McLoughlin

III. 2006: HSARPA/SBIR; 1.1 DHS S&T TOPICS; SBIR/STTR TOPIC NUMBER: H-SB06.2-003; TITLE: ADVANCED UNATTENDED GROUND SENSOR (UGS) TECHNOLOGIES. Abstract for Review to the Attention of: Ms. Leslee Shumway

IV. 2006: SBIR/STTR, SWIFT Tour September, 2006; Topic: Ten federal agencies collaborate to sponsor the 2006 SWIFT Tour; Executive Summary submitted to each Federal agency participating in the SWIFT Tour included NIH, DOT, NSF, DOE, Navy, Air Force, Army, DARPA, DoD, Chem-Bio Defense, NASA, and the DHS. Deborah Akwei at (202) 889-5064.

V. 2006: DHS/HSARPA/SBIR Science and Technology (S&T) Directorate Topic: High risk, high payoff R&D initiatives Executive Summary/Proposal submitted by E-mail correspondence to: Ms. Elissa (Lisa) Sobolewski; DHS/SBIR Program Manager

VI. 2007: DHS; S&T Directorate Borders and Maritime Division Topic: "White Paper" Submission for SAFECON (BAA07-02A); RFI Submitted to the attention of: Margo L. "Margo" Graves; Team Lead / Contracting Officer

VII. 2007: U.S. Army/ECBC; Topic: ECBC agreed to develop chemical, biological, and explosives detectors, under the SAFECON BAA. Collaborative Agreements with: Daniel M. Nowak; Program Manager. Contact: 410-436-5631; daniel.nowak@us.army.mil. Dr. Augustus W. Fountain III; Chief Scientist. Contact: 410-436-0683; augustus.w.fountain@us.army.mil

VIII. 2007: Senate Committee on Homeland Security and Governmental Affairs. Topic: Container Security: "White Paper" Submission for DHS; SAFECON Project; RFI Letter sent to the Attention of: Joe Lieberman; Chairman Senate Committee on Homeland Security and Governmental Affairs, 340 Dirksen Senate Office Building, Washington, D.C. 20510

IX. 2007: US Naval Research Laboratory (NRL); Topic: Biochemical, and logistical preparations to integrate a biosensor with an appropriate air collector. Collaborative Agreements with: Chris R. Taitt; Program Manager. Contact: 202-404-4208; chris.taitt@nrl.navy.mil; Paul T. Charles; Contact person. Contact: 202-404-6064; paul.charles@nrl.navy.mil

X. 2007: DOE/ORNL Topic: Oak Ridge National Laboratory agreed to develop Chemical, Explosive, Radiological, and Nuclear detectors. Collaborative Agreements with: Blair Ross; Program Manager Contact: 865-576-1034; rossb@ornl.gov. Richard L. Stouder; Contact Person. Contact: 865-574-3053; stouderrl@ornl.gov

XI. 2007: DHS; S&T Directorate Office of Procurement Operations. Topic: "White Paper" Submission for *"CELL-ALL Ubiquitous Biological and Chemical Sensing"* (BAA07-10); RFP. Submitted to the attention of: Margo L. "Margo" Graves; Team Lead / Contracting Officer

XII. 2007: During the year 2007, several conversations were held with Jim Culbertson (On-Star); General Motors Global Process Leadership in Warren, MI; General Motors Research and Development (R&D) Center; and, General Motors Technology Portal, Silicon Valley, CA. A letter was also sent to the Chairman & CEO of General Motors, G. Richard Wagoner, informing Mr. Wagoner that the General Motors "Stolen Vehicle Slowdown System" the company announced in October, 2007, is in fact the same system I discussed with several of its employees during the year 2007. A copy of the letter written to the Chairman and CEO of General Motors:

ATPG TECHNOLOGY, LLC
Anti-Terrorism Product Grouping
Larry Golden, CEO
522 Peach Grove Place, Mauldin, SC 29662
E-mail: lgolden5605@charter.net; E-mail: atpg-tech@charter.net
Bus. 864-288-5605 / Mobile: 864-320-0012

April 14, 2008

General Motors Corporation
G. Richard Wagoner, Jr, Chairman & CEO
P.O. Box 33170
Detroit, MI 48232-5170

Dear Mr. Wagoner:

I've made several attempts to contact Representatives of GM. I talked with and forwarded information to a few Representatives of both OnStar and GM last year during the months of March and April of 2007.

I shared with them technology I had at that time "patent pending" that is designed to stop moving vehicles. I wanted OnStar and GM to collaborate with me in responding to a Government solicitation.

I tried again to contact OnStar and GM when you made the announcement on October 8, 2007 of having technology that will stop moving vehicles which caused your share price to move upward $4 dollars over the next 4 days (value, $2.2 billion).

I need to know if you have a patent for the technology. If you do, please send that information to me. My Patent Attorney and the PTO didn't find one. My patent application and all the claims have been allowed by the PTO.

If I don't hear back from you in a couple of days, my plans are to do a cease-and- desist for the 2 million, 2009 vehicles you have scheduled to roll out with that technology.

Thanks,
Larry Golden
Larry Golden, CEO

PREVENTING VEHICULAR TERRORIST ATTACKS WITH A STALL, STOP, VEHICLE SLOWDOWN SYSTEM

Patent Claim A vehicle adapted for receipt of a signal from a remote location to remotely control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein a user determines that the vehicle has been stolen and in response initiates a distress signal communication over a communication network that causes communication between the vehicle and the remote location and that then causes the at least one control signal to be sent from the remote location via the communication network that includes at least one of a cell phone tower and a satellite.

XIII. 2008: DHS; S&T Directorate Topic: “Read-Ahead” request made by Edward Turner prior to a face-to-face meeting at DHS. Subject matter: “Multi detection; Cell phone detection; Lock disabling; and, Stall-to-Stop “Read-Ahead” document submitted to; and face-to-face meeting held with: Edward Turner; DHS Program Manager. Doug Lane; DHS Liaison

XIV. 2008: DHS S&T LONG RANGE BROAD AGENCY ANNOUNCEMENT (BAA08-01). Topics: Cargo Container Security Device; Cell Phone Detection System; Stall-to-Stop Device "White Paper" submitted to the attention of: David Newton; Acting Division Head, Borders and Maritime Division. Contact: S&T-BordersMaritime@dhs.gov

XV. 2008: DoD/DARPA Strategic Technologies Office; (BAA) 08-10. Topic areas: 1- WMD Defense; 2- Small Unit Operations; 3- Maritime Operations; 4- Core Strategic Technologies. Submitted: A one-page "Executive Summary" via the web-based TFIMS application at http://www.tfirms.darpa.mil/baa

XVI. 2008: DHS; S&T Directorate Office of Procurement Operations "TRUST" INDUSTRY DAY. Topic: A device to detect WMD threats, Contraband; CBRNE substances contained within a maritime shipping container. Panel discussion and Proposal submission: Dave Masters; "TRUST" Program Manager

XVII. 2009: DHS; S&T Directorate Office of Procurement Operations Topic: "White Paper" Submission for "TRUST" solicitation RFI. Submitted to the attention of: Emily Graham, Contract Specialist. Contact: 202-254-5611; Emily.graham@dhs.gov

XVIII. 2009: DHS; S&T Directorate Office of Procurement Operations. Topic: Proposal Submission for *"CELL-ALL Ubiquitous Biological and Chemical Sensing"* (BAA07-10); E-mail correspondence and proposal to: Stephen Dennis, Program Manager http://cellall.webcaston.tv/home/homepage.php>

XIX. 2009: DHS; S&T Directorate. Topic: "TRUST" (BAA) 09-17: A device to detect WMD threats, Contraband; CBRNE-H substances contained within a maritime shipping container. Full proposal submission made to the attention of: Director of Innovation. Contact: BAA09-17@hq.dhs.gov

XX. 2009: DHS LEGISLATIVE AFFAIRS. Topic: Letter of support sent from the Honorable Congressman Bob Inglis office 4th District of South Carolina in reference to the "TRUST" project. Letter sent to: Eddie Gleason, DHS Director; OLA

XXI. 2010: Subcommittee on Emerging Threats, Cybersecurity, Science and Technology. Topic Area: CBRNE Security Meeting Request with U.S. Representative Yvette D. Clarke 1029 Longworth HOB Letter sent to the Attention of: Algene Sajery FBO / U.S. Representative Yvette D. Clarke, 1029 Longworth HOB, Washington, DC 20515

XXII. 2010: DHS; S&T Directorate (LRBAA10-01). Borders and Maritime Division. Topic: Border Security; Maritime Security; Cargo Security. Title of "White Paper" proposal: "Integrated Systems for Border and Maritime Security". "White Paper" submitted to: SandT-BordersMaritime@dhs.gov

XXIII. 2011: DHS; S&T Directorate (LRBAA10-01).Borders and Maritime Division. Topic: Border Security; Maritime Security; Cargo Security; Title of "White Paper" proposal: "Integrated Systems for Border and Maritime Security". Response Letter from: Cherita Thomas, Associate Director/Contracting Officer. Department of Homeland Security Office of Procurement Operations Science and Technology Acquisition Division

XXIV. 2011: White House Office of Science and Technology Policy. Executive Office of the President. Topic Area: Brake Override System. Letter sent to the Attention of: Aneesh Chopra, U.S. Chief Technology Officer, 725 17th Street Room 5228, Washington, DC 20502

XXV. 2011: Larry Golden's written Testimony Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package*. Prepared for: The Honorable Aneesh Chopra U.S. Chief Technology Officer White House Office of Science and Technology Policy Executive Office of the President

XXVI. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package*. Prepared for: The Honorable David L. Strickland Administrator National Highway Traffic Safety Administration

XXVII. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package*. Prepared for: Committee on Energy and Commerce Subcommittee on Oversight and Investigations U.S. House of Representatives

XXVIII. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package*. Prepared for: The Honorable Trey Gowdy S.C. Representative; District Number 4. U.S. House of Representatives

XXIX. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package*. Prepared for: The Honorable Nikki Haley, Governor S.C. Office of the Governor

XXX. 2013: Secretary's Office of DHS. Submissions made to: Ms. Janet Napolitano, Secretary of DHS. Mr. Ivan K. Fong, General Counsel of DHS

BORDER SECURITY

SBInet was a program initiated in 2006, created under U.S. Customs and Border Protection to design a new integrated system of personnel, infrastructure, technology, and rapid response to secure the northern and southern land borders of the U.S. DHS decided to have development of SBInet managed by a single private contractor.

On September 21, 2006 DHS announced the award of the SBInet contract to Boeing. Boeing, holding the primary contract, subcontracted many portions of the design, development, implementation, and maintenance of the program, while Boeing handled the majority of the management aspects.

SBInet was controlled by an indefinite delivery/indefinite quantity contract extending through September 30, 2009, with three one-year option periods. The only commitment DHS

made was to pay for a 28-mile pilot section of SBInet in the Tucson sector of the Arizona-Mexico border. The cost of the pilot section was estimated at $67 million. The value of Boeing's three-year contract to build SBInet across both the northern and southern borders was estimated by various sources at various times to be between $2 billion and $8 billion. The technology included:

Tower system: Towers were meant to be set up along the border, with varying surveillance and communications equipment. Towers were slated to include radar, long-range cameras, broadband wireless access points, thermal imaging capabilities, ground sensors, and motion detectors.

Command centers: All of the information received by sensors were meant to go to command centers, where a "common operating picture" would have been compiled and shared with other agencies. The common operating picture would have appeared on computer screens as a geospatial map, where border entries are tracked in real time. Command center personnel were supposed to be able to click on a given entry, view the entry, and assess the threat using the long-range cameras on the towers.

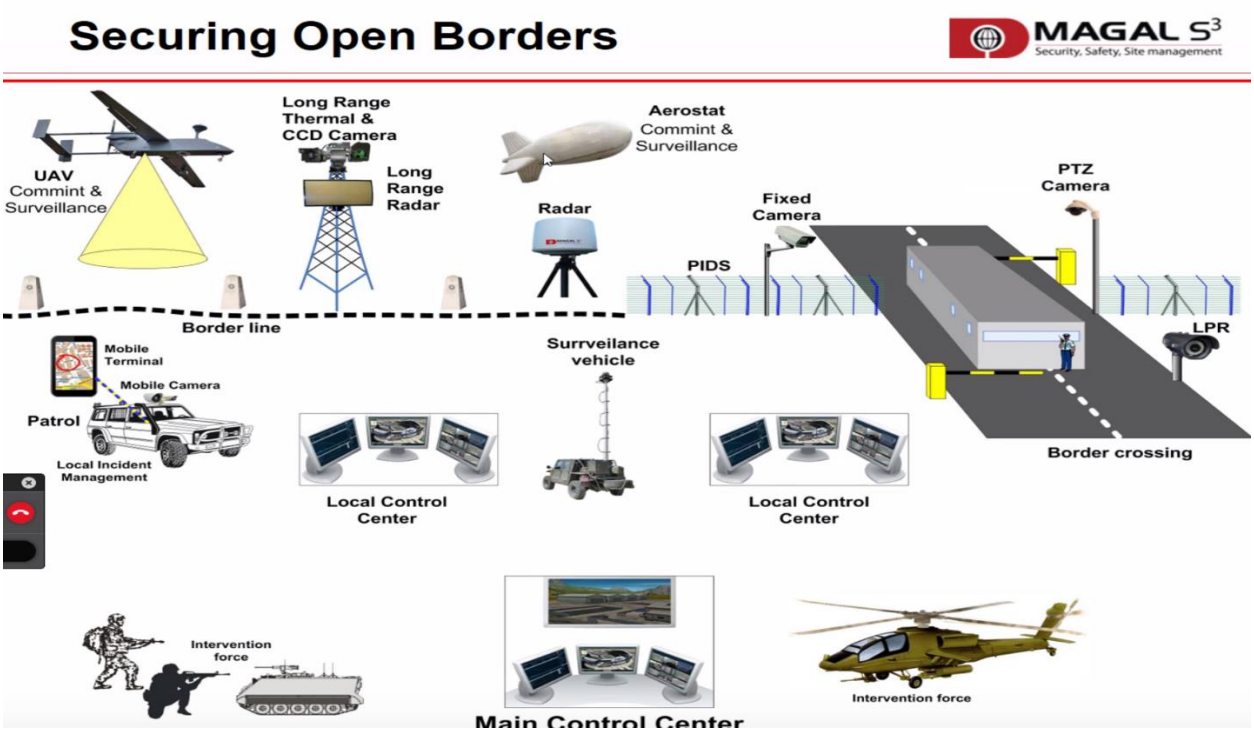
Border Patrol response: Border Patrol agents were meant to carry PDAs with GPS capabilities, to allow the command center to track the location of agents prohibiting illegal entries and watch the encounter in real time on the common operating picture. Additionally, the PDAs were supposed to have advanced finger print identification technology, to allow Border Patrol agents to identify an individual at the prohibition site immediately and the ability to view and control tower cameras from their PDA. In addition, Border Patrol agents will be given laptops in the patrol car.

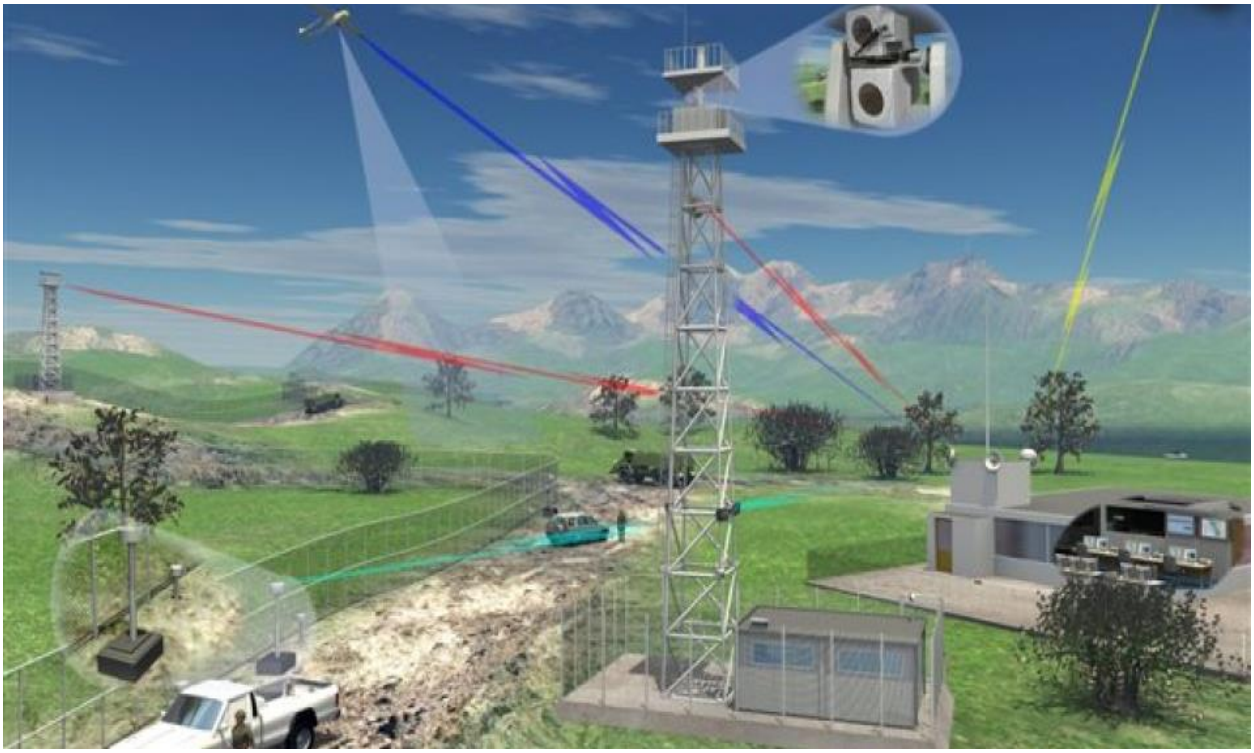
Airborne sensors: Airborne sensors on unmanned aerial vehicles (UAVs) were meant to fill in gaps in the "virtual fence" in remote areas where building and maintaining towers was impractical.

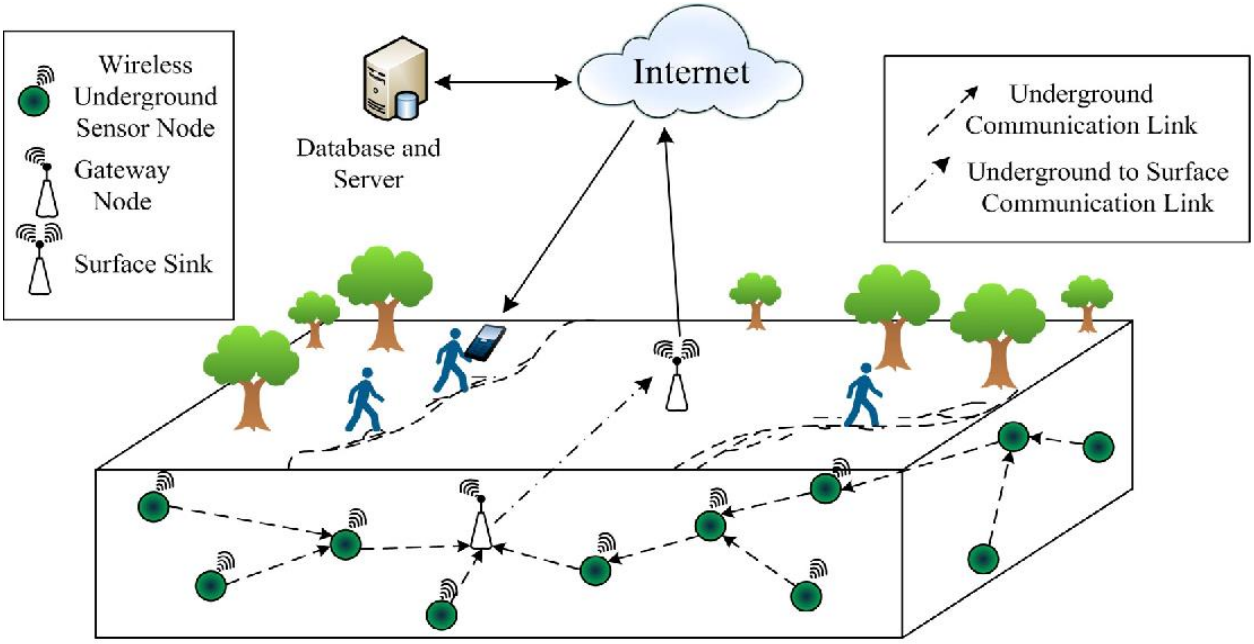
Janice Kephart of the Center for Immigration Studies defended SBINet, writing, "SBInet is still operational where it was deployed, despite the widespread notion that the light switch was turned off. She stated, "the reason SBInet is still operating is because it works".

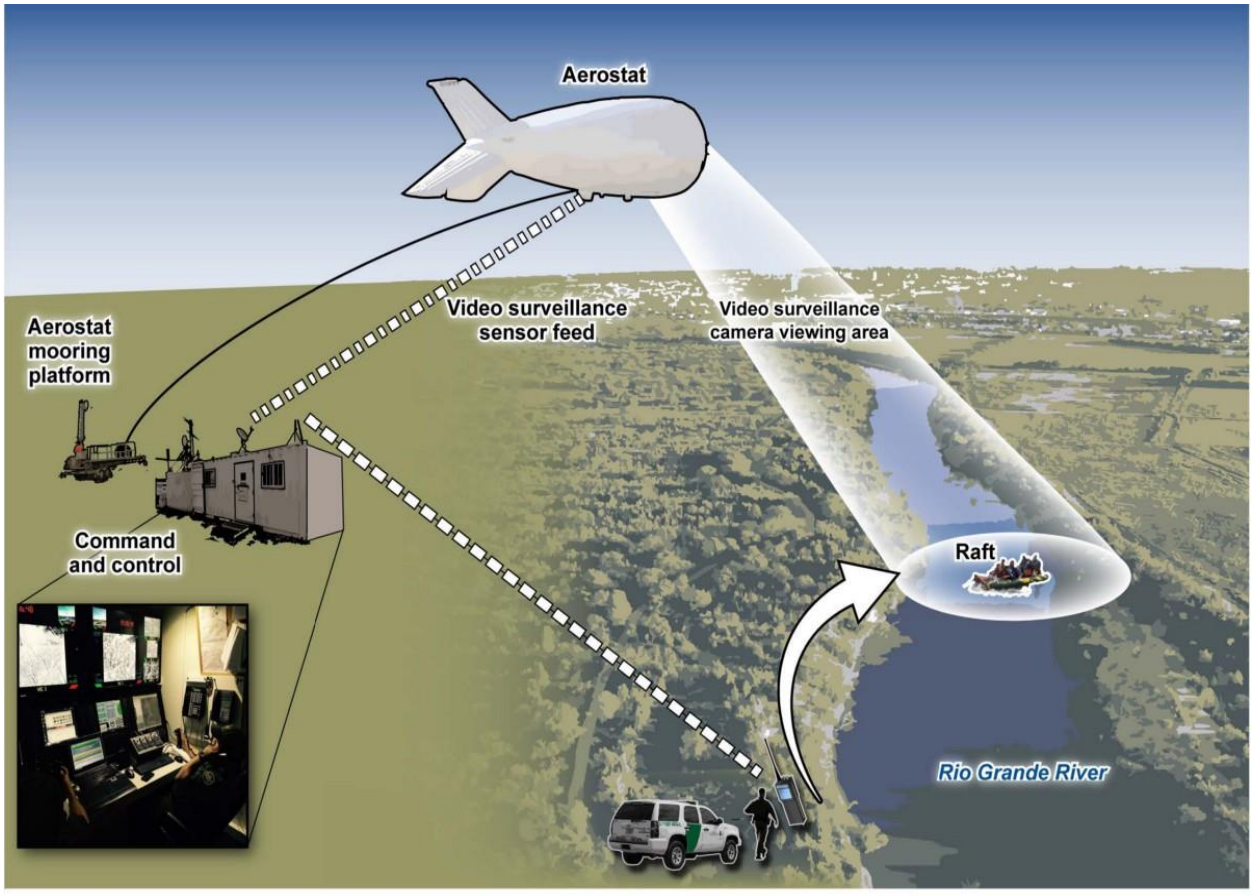
DHS Secretary Janet Napolitano ordered an assessment of the project in January 2010 and in March 2010 froze additional funding. On Jan. 14, 2011, DHS said it would redirect

funding originally intended for SBInet—including fiscal 2011 SBInet funds—to the new border security technology effort.









Source: GAO analysis of U.S. Customs and Border Protection (CBP) information; CBP (photos). | GAO-17-152

Patent Claim A multi sensor detection system capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities vulnerable to terrorist activity that can be integrated with and interconnected to watchtowers to form a network, comprising:

at least one of an integrated watchtower, a fixed watchtower, a surveillance watchtower, a watchtower capable of scanning, a watchtower capable of monitoring, a watchtower equipped with sensors or a watchtower interconnected to a central monitoring terminal for sending signals thereto and receiving signals therefrom;

wherein the at least one watchtower is equipped with a remote video surveillance camera that provides at least one night vision means of surveillance or an infrared human detection means of surveillance capability and is integrated into a watchtower's remotely controlled system that can monitor, detect, track, and identify humans;

a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop personal computer (PC), a notebook personal computer (PC), a laptop, a satellite phone, a smart phone, a cell phone, a Universal Mobile Telecommunications System (UMTS) phone, a personal digital assistant (PDA), a liquid crystal display (LCD) monitor, a satellite, or a handheld, interconnected to a monitoring equipment for sending signals thereto and receiving signals therefrom;

a communication method of at least one of a Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), or central processing unit (CPU), used to interconnect the communication device to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a plurality of sensors for detecting or sensing humans that is at least one of a chemical human sensor, biological human sensor, radiological human sensor, infrared human detector, motion human detector, or image human detector, interconnected to or disposed within the multi-sensor detection system for sending signals thereto and receiving signals therefrom;

a mobile multi-sensor detection device that is at least one of a ground surveillance sensor,

a surveillance radar sensor, a surveillance camera, or a stand-alone surveillance scanner, that is mounted in, on, or upon at least one of a car, a truck, a camper, a bus, a van, an unmanned aerial vehicle (UAV), an unmanned ground vehicle (UGV), or a utility vehicle, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a hand-held multi-sensor detection device that is capable of at least one of thermal imaging or infrared imaging for monitoring, detecting, tracking and identifying humans, that is controlled or operated by at least one authorized person who is an owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, or monitoring site and terminal personnel, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, wherein the authorized person manually initiates the signal to the monitoring equipment to alert upon the monitoring, detecting, tracking and identifying of the human;

whereupon, detection by the mobile multi-sensor detection device causes an automatic signal transmission to be sent to, or received from, any products in product grouping categories of storage and transportation, sensors, detector case; modified and adapted, monitoring and communication devices, communication methods, biometrics;

whereupon, detection of an unauthorized vehicle, an unauthorized driver or operator of a vehicle or mobile unit, a signal is sent from the communication device to the vehicle or mobile unit to stop, stall or slowdown the vehicle;

wherein, a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop PC, a notebook PC, a laptop, a satellite phone, a smart phone, a cell phone, a UMTS phone, a PDA, a LCD monitor, a satellite, or a handheld, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, comprising a lock disabling mechanism that is able to engage (lock), and disengage (unlock) and disable (make unavailable) after a specific number of tries.

Patent Claim The multi sensor detection system of claim 1, capable of identifying,

monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities, further includes the identifying, monitoring, and detecting of terrorist, that is at least one of an illegal, radical, fanatic, activist, revolutionist or rebel.

Patent Claim The multi-sensor detection system of claim 1, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The multi-sensor detection system of claim 1, further includes a navigation system adapted for communication with at least one of the surveillance watchtowers.

Patent Claim The multi-sensor detection system of claim 1, capable of forming a wired or wireless sensor network.

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The multi-sensor detection system of claim 1, capable of being embedded into; placed in, on, or adjacent to at least one of the products in the product grouping categories or an area targeted for monitoring.

Patent Claim The multi-sensor detection system of claim 1, capable of sending signals thereto and receiving signals therefrom to engage (lock), disengage (unlock) and disable (make unavailable) a lock after a specific number of tries that is interconnected to the multi sensor detection system or monitoring equipment.

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi-sensor detection system of claim 1, interconnected with a camera to

view the environment in real-time or to store the data for transmission and review at a later time.

Patent Claim The multi-sensor detection system of claim 1, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

UNMANNED AERIAL VEHICLE (UAV) / UNMANNED GROUND VEHICLE (UGV)

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.

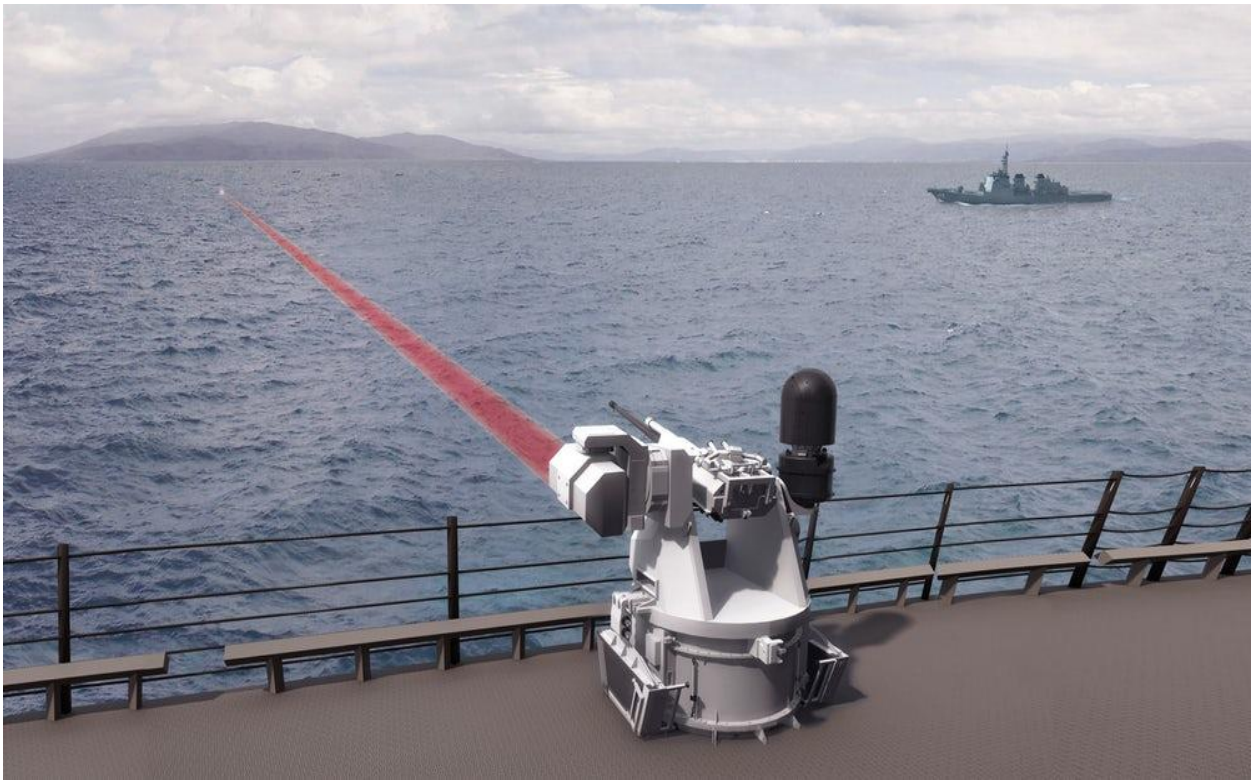
Patent Claim The multi-sensor detection and automatic/mechanical lock disabler system of claim 12 wherein the cell phone detector case includes telecommunication and radio communication means that are interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships, UAVs, UGVs, and airplanes.

Patent Claim The communication device of claim 11 wherein the communication device includes telecommunication, telematics, long and short range radio frequency communication

means that are interactive with any type of motive vehicle that includes, but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships, UAVs, UGVs, and airplanes.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case includes telecommunication, telematics, long and short range radio frequency communication means that are interactive with any type of motive vehicle comprising a car, truck, van, SUV, train, subway, boat, ship, UAV, UGV, or airplane.

ELECTROMAGNET PULSE, ELECTROSTATIC DISCHARGE, MICROWAVE BEAM OR RADIO FREQUENCY TO STALL, STOP, OR SLOW-DOWN A VEHICLE



Patent Claim A vehicle adapted for receipt of a signal from a remote location to control the vehicle's stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the at least one control signal is sent due to unauthorized use of the vehicle, and wherein an originating first signal that eventually causes the at least one control signal to be sent is generated upon initial verification of the unauthorized use of the vehicle;

at least one mobile, portable, or fixed device capable of sending the at least one control signal from the remote location that is of electromagnet pulse, electrostatic discharge, microwave beam or radio frequency, to disable the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and horsepower of the motor.

AUTONOMOUS VEHICLE EQUIPPED WITH AN ELECTROMAGNET PULSE, ELECTROSTATIC DISCHARGE, MICROWAVE BEAM OR RADIO FREQUENCY TO STALL, STOP, OR SLOW-DOWN A VEHICLE

Patent Claim A vehicle adapted for receipt of a signal from a pre-programmed automated system to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the receivers, the computer system, and the electrical system are part of at least one pre-programmed operating system of unintended acceleration, pre-crash, reverse acceleration, stabilization, lane departure, cruise control, driverless vehicle, and chemical biological radiological nuclear explosive (CBRNE) detection;

wherein the control signal to activate the stall-to-stop or vehicle slowdown is not remote from the vehicle and the signal to activate is initiated when at least one of the vehicle's operating systems for monitoring the vehicle's condition exceeds a pre-programmed vehicle operating system parameter.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, pre-programmed automated system further including a cellular communication device adapted for communication with at least one cell phone tower; further including, at least one satellite connection capable of communicating with the pre-programmed automated system; further including, at least one modem connection for short and long range radio frequency transmissions with the pre-programmed automated system.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system

and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is an in-vehicle notification warning of: crash, vehicle parking, speeding; driving too fast for conditions; construction zone; school zone; accident ahead; brake failure; acceleration/deceleration failure; acceleration/deceleration cruise control.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when the vehicle is in forward movement, backward or reverse movement, side movement, cruise control movement, or lane departure movement or when the vehicle moves outside a designated perimeter or zone.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is a detection of a bomb, weapon of mass destruction, chemical or biological agents, located in, on, or adjacent to a vehicle.

MARITIME CARGO CONTAINER DETECTION DEVICE

Patent Claim A maritime cargo container multi-sensor detection system for monitoring products and for detecting at least one explosive, nuclear, contraband, chemical, human, biological, or radiological agents so that terrorist activity can be prevented, comprising:

a plurality of sensors for detecting the at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and capable of being disposed within a multi-sensor detection device;

monitoring equipment located at a determinate site that is remote from the maritime cargo container and not in contact with the maritime cargo container, to include, but is not limited to at least one of computers, laptops, notebooks, PCs, handhelds, readers, cell phones, PDAs or smart phones for the receipt and transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

at least one satellite capable of transmitting signals to the monitoring equipment and receiving signals from the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication with the maritime cargo container multi sensor detection device;

at least one modem for short and/or long range radio frequency communication with the maritime cargo container multi sensor detection device;

at least one interface for establishing a remote, global communications and tracking network that works with the maritime cargo container multi-sensor detection device;

at least one internet connection capable of communication between the maritime cargo container multi sensor detection device and the monitoring equipment;

whereupon a signal sent from a maritime cargo container multi sensor detection device to a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes the transmitting of location data and sensor data.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of forming a wired or wireless sensor network.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of forming a mesh network for redundancy.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the power source is electrical, battery, solar, or a combination thereof.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of being embedded into; placed in, on, or adjacent to a product or area targeted for monitoring.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of sending signals thereto and receiving signals therefrom to lock, disable a lock, enable a lock, or unlock a lock that is interconnected to the multi sensor detection device and monitoring equipment.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of transmitting biometric and authentication data include, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, interconnected with a camera to view the environment in real-time or to store the data for transmission and review at a later time.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56,

interconnected with a camera; light and video sensors to allow the user to view the environment from a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the maritime cargo container multi-sensor detection device is capable of receiving signals and messages from, and sending signals and information to, at least one of; a remote lock, a remote communication device, a vehicle and another multi-sensor detection device.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the maritime cargo container multi-sensor detection device is capable of communicating through a physical interface.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of a unique ID number with authentication; timing/location signal; sensor status; battery condition, stored sensor messages, and can alert a remote monitor.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of monitoring and allowing transmission and propagation of containers while stacked, either afloat or ashore.

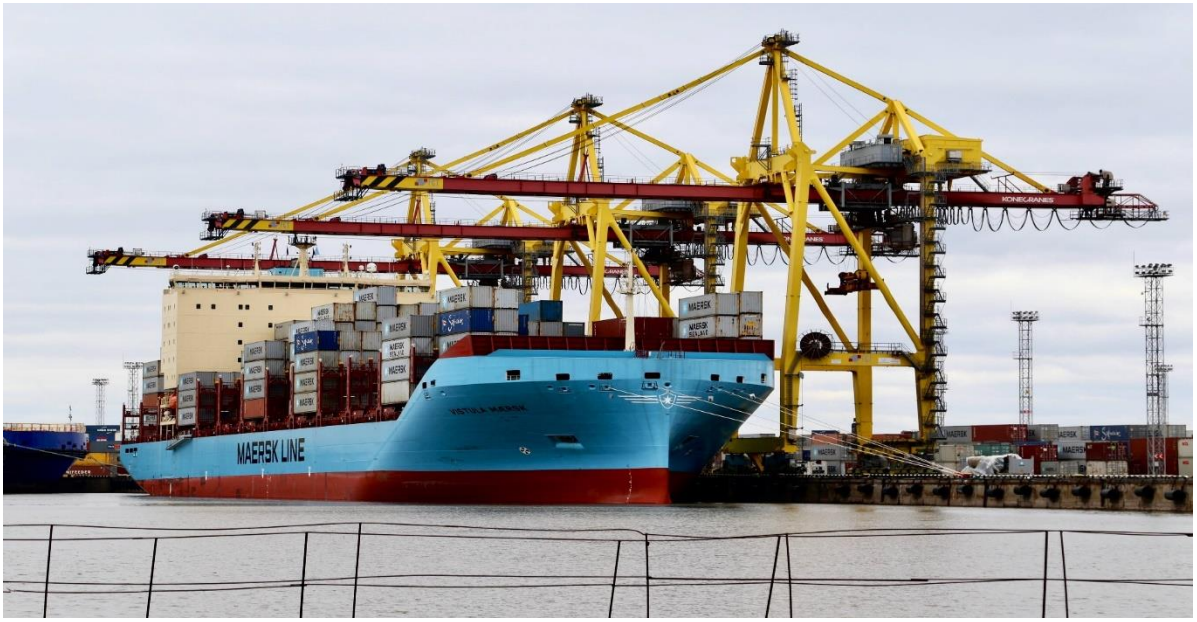
Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of having interfaces with environmental and security sensors and is able to interrogate and pass data from the sensors.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of capable of communicating a security alert globally through the use of radio frequency, cellular and satellite technology.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of sending signals and messages to; receiving signals

and messages from; at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation or monitoring site.

SEAPORT CRANE, HARBOR CRANE OR STRADDLE-CARRIER



Patent Claim A maritime cargo container multi-sensor detection system for monitoring and for detecting at least one explosive, nuclear, human, contraband, chemical, biological, or radiological agents and compounds so that terrorist activity can be prevented, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds;

monitoring equipment located at a determinate site that is remote from the maritime cargo container and not in contact with the maritime cargo container, that is at least one of a computer, laptop, notebook, PC, handheld, transceiver, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;

at least one of a modem for short and/or long range radio frequency, a cellular connection, a Wifi connection, a satellite connection, an interface connection, or an internet connection, interconnected to the monitoring equipment for sending signals and messages thereto and receiving signals and messages therefrom;

a maritime cargo container multi-sensor detection device that is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of loading, offloading, or transport within the seaport terminal facility;

whereupon a signal sent from the maritime cargo container multi sensor detection device to a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data.

Patent Claim The multi-sensor detection system of claim 136, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The multi-sensor detection system of claim 136, capable of forming a wired or wireless sensor network.

Patent Claim The multi-sensor detection system of claim 136, capable of forming a mesh network for redundancy.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, wherein the power source is electrical, battery, solar, or a combination thereof.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of sending signals thereto and receiving signals therefrom to lock, disable a lock, enable a lock, or unlock a lock that is interconnected to the maritime cargo container multi sensor detection device and monitoring

equipment.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of transmitting biometric and authentication data that includes, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation or a monitoring site.

A COMMUNICATING, MONITORING, DETECTING, AND CONTROLLING (CMDC) DEVICE FOR BORDER SECURITY

CMDC DEVICE / BIOMETRIC DATA BASE FOR REGISTERING IMMIGRANTS

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi sensor detection security systems of claim 145, further including biometrics of at least one of, but not limited to fingerprints, iris, signature and voice to prevent entry or exit of unauthorized persons.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

Patent Claim The multi-sensor detection system of claim 81, wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The communication device of claim 11 wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals

CMDC DEVICE / HOME, BUILDING, AND CARGO CONTAINER LOCKS

Patent Claim Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to at least one of a home lock, a building lock, or a cargo container lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a home lock, a building lock, or a cargo container lock;

a receiver for receiving signals from at least one of a home lock, a building lock, or a cargo container lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RE) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long

range radio frequency (RF) connection, short range radio frequency (RE) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and,

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a home lock, a building lock, or a cargo container lock whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the home lock, building lock, or cargo container lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

CMDC DEVICE / UNMANNED AERIAL, LAND, SEA VEHICLE LOCKS

Smartphone Controlled Drone Market

Patent Claim Monitoring equipment that is at least one of products grouped together by

common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal, digital assistant (PDA) or smart phone interconnected to a vehicle lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a receiver for receiving signals from at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RF) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and,

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the manned or unmanned aerial vehicle lock, manned or unmanned ground vehicle lock, or manned or unmanned sea vehicle lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

CMDC DEVICE / INTERNET OF THINGS (IoTs) FOR BORDER SECURITY

Patent Claim A monitoring equipment, comprising:

at least one central processing unit (CPU);

at least one motion sensor in communication with the at least one CPU;

at least one light indicator in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

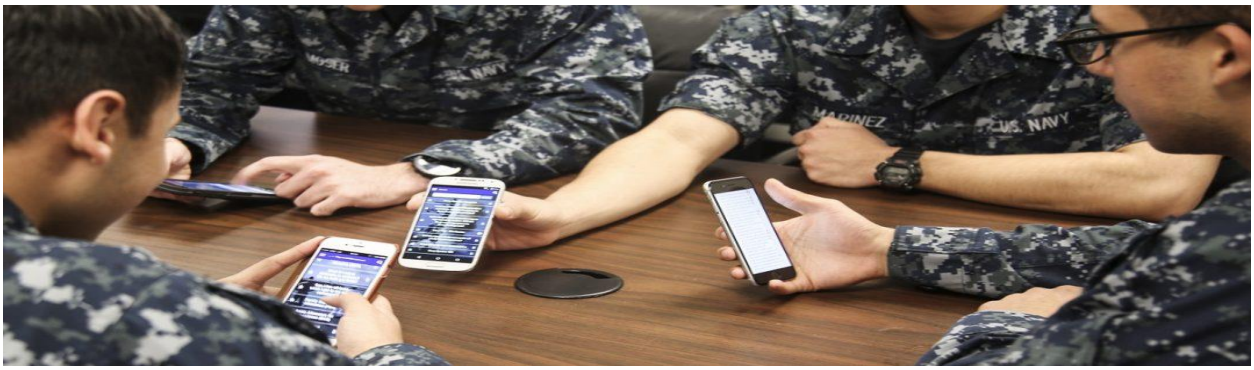
at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;

at least one or more detectors in communication with the art least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

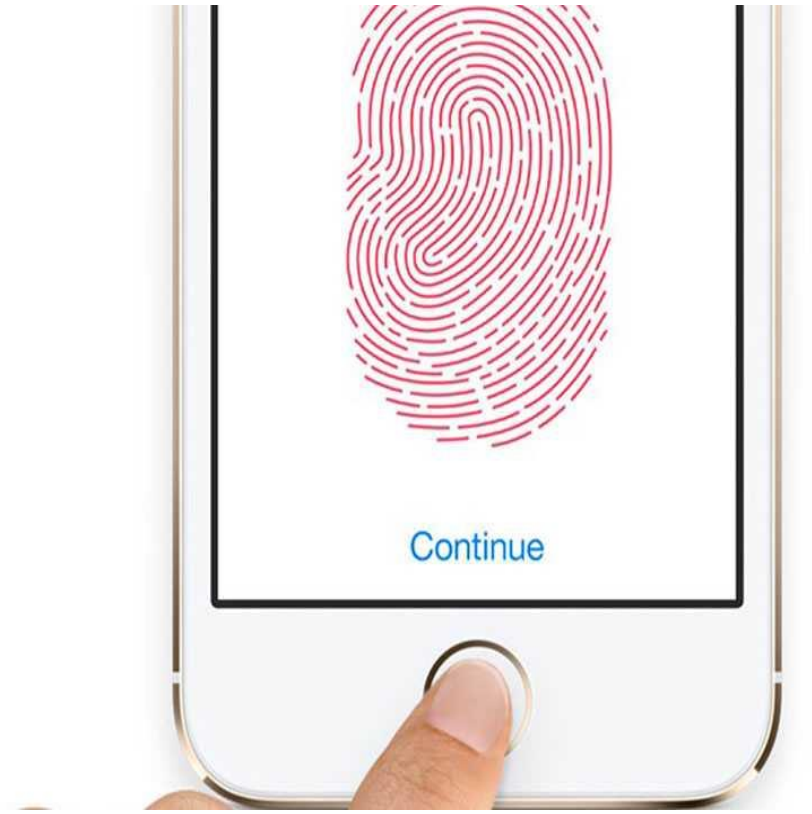
at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the **communication device is capable of communicating, monitoring, detecting, and controlling.**

CMDC DEVICE / FOR MILITARY AND BORDER SECURITY PERSONNEL



Patent Claim The communication device of claim 11 wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.

CMDC DEVICE / ENABLES (MAKE AVAILABLE) THE CMDC DEVICE AFTER A BIOMETRIC FINGERPRINT OR FACIAL AUTHENTICATION IS MADE TO THE DEVICE BY AN AUTHORIZED USER (The first smartphone with a fingerprint reader was the Motorola Atrix 4G in 2011)



Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of communicating, monitoring, detecting, and controlling.**

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

CMDC DEVICE / LOCATION FOR THE CMDC DEVICE ITSELF; INTERCONNECTED TO THE MULTI SENSOR DETECTION DEVICES; THE STALL TO STOP SYSTEMS; AND, THE LOCKING MECHANISMS

Apple Location Services allows Apple and third-party apps and websites to gather and use information based on the current location of your iPhone or Apple Watch to provide a variety of location-based services. To use features such as these, you must enable Location Services on your iPhone and give your permission to each app or website before it can use your location data. Location Services uses GPS and Bluetooth (where those are available) along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your device's approximate location. Your Apple Watch may use the location of your paired iPhone if it is nearby.

If Location Services is on, your iPhone will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple, to be used for augmenting this crowd-sourced database of Wi-Fi hotspot and cell tower locations.

By enabling Apple's Location Services, location-based system services such as these will also be enabled:

- **Traffic**: If you are physically moving (for example, traveling in a car), your iPhone will periodically send GPS locations and travel speed information in an anonymous and encrypted form to Apple, to be used for augmenting a crowd-sourced road traffic database.
- **Significant Locations**: Your iPhone will keep track of places you have recently been, as well as how often and when you visited them. This data is encrypted and stored only on your device and will not be shared without your consent. It is used to provide you with personalized services, such as predictive traffic routing.
- **Location-Based Suggestions**: If you turn off Location Services for Location-based Suggestions, Apple may use the IP address of your internet connection to approximate your location by matching it to a geographic region.
- **Location-Based Alerts**: Your iPhone and Apple Watch will use your location in order to provide you with geographically-relevant alerts, such as a reminder to call someone when you get to a specific place.
- **Share My Location**: You can choose to share your current location with others, on a temporary or ongoing basis, from within certain apps such as Messages and Find My Friends.
- **HomeKit**: Your iPhone will use your location to enable accessories to turn on or off when you arrive at or leave a specific location, such as turning on your lights when you get home.
- **Emergency Calls & SOS**: When you make an emergency call, in addition to location already provided to emergency services, your iPhone will make supplementary location data available through the Enhanced Emergency Data service, where supported. In addition, triggering emergency SOS will send location to your emergency contacts at the end of the call.

Ouote from the "CellAll" Proposal submitted to the DHS in 2007, "Initially the SMD will look to the on-board GPS (if provided) to determine position. If the cell phone is equipped with a GPS the application on the cell phone will retrieve the position from its own GPS. When a GPS position cannot be determined, the position of the SMD and its user will be calculated based on a cell phone tower database, provided by the FCC and signal strength. If this does not yield a result, the Wi-Fi hotspot database will be utilized to determine SMD and user position. If all these options fail, the last known position can be augmented with the on board accelerometers to

estimate the current position which will be reported to the control centers and annotated as a last position and a possible position."

Patent Claim The communication device of claim 11 wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

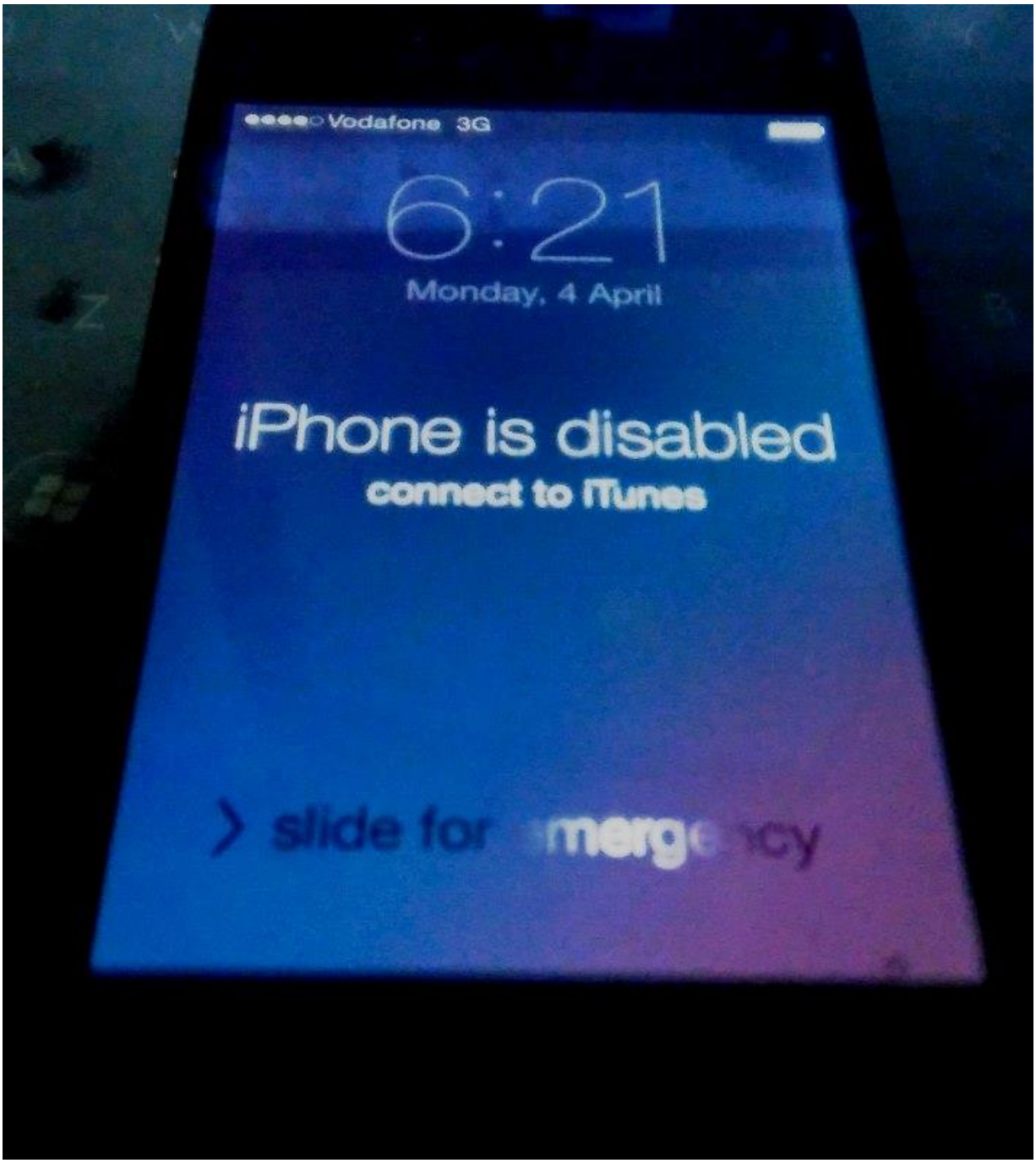
Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case have at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, or a GPS connection.

Patent Claim The multi-sensor detection system of claim 125 wherein the internal or external remote/electrical lock disabler includes at least one of: a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are interconnected to the central processing unit (cpu).

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 11, wherein a communication link is present of at least one of a Wi-Fi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device includes at least one of; a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are capable of being interconnected to a central processing unit (cpu) of the communication device.

CMDC DEVICE / DISABLE (MAKE UNAVAILABLE) THE CMDC DEVICE AFTER MULTIBLE FAILED ATTEMPTS TO DENY ACCESS TO THE DEVICE BY UNAUTHORIZED USERS (In 2014, Apple's "Find my iPhone" and Google's "Android Device Manager" can locate, disable, and wipe the data from phones).



Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of**

communicating, monitoring, detecting, and controlling.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to lock, or disable the lock of the product thus preventing further contamination and denying access to the product by unauthorized, untrained, and unequipped individuals.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed for outside and/or inside of the products listed in the product grouping.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device can be used with cars, trains, airplanes, ships and any of the products listed in the product groupings.

CMDC DEVICE / RADIO FREQUENCY NEAR FIELD COMMUNICATION (NFC); A BETTER CHOICE FOR RADIO FREQUENCY (RF) COMMUNICATION WHEN COMPARED TO RADIO FREQUENCY IDENTIFICATION (RFID)

RFID Signals can Detonate Bombs in Cargo Containers: But How Serious is the Vulnerability?

August 10, 2011 Homeland Security Today

In the fall of 2007, a handful of officials from the Department of Homeland Security (DHS) were invited to attend a live demonstration of how a bomb hidden inside a commercial cargo container could be detonated by a homemade radio frequency identification (RFID) container tracking tag operating at a frequency that was mandated by the federal government for cargo containers within US port environments.

A cargo container RFID electronic tag, or seal, contains an electronic reader that receives a port's RFID signal that prompts the container's RFID tag to transmit to port authorities' data regarding the cargo that's been encoded on its RFID tag. But as the

demonstration showed, it also can be used to close an electronic circuit when it receives a corresponding RF from a port RFID sender/receiver, thereby detonating the bomb. Indeed. In the November, 2007 test, an RF receiver tuned to pick up a required US port RFID reader frequency triggered the small explosive that had been placed inside the empty container.

What's important about the demonstration is that the homemade RF receiver was operating at a frequency that not only was mandated to be used within port environs, but also was mandated to be made public despite the fact that "the process of selecting a frequency for container security was contentious," *Homeland Security Today* was told by Powers Global Holdings, Inc. Chairman, a former FBI agent who worked with CBP on border related security issues while in Laredo, Texas.

RFID systems consist of a reader with an antenna, and a transponder (tag). There are two different RFID tags possible. Either they are active, meaning they have their own power source or they are passive. Passive tags have no own power source and have to be supplied with energy via an electromagnetic field produced by the reader.

NFC stands for Near-Field Communication. NFC is also based on the RFID protocols. The main difference to RFID is that a NFC device can act not only as a reader, but also as a tag (card emulation mode). In peer-to-peer mode, it is also possible to transfer information between two NFC devices. Because of the short read range limitations, NFC devices have to be in very close proximity - usually no more than a few centimeters. That's why NFC is often used for secure communications.

NFC is almost exclusively used for high-speed data transfer between two electronic systems, like a smartphone and a payment reader in the checkout line, or two smartphones exchanging data, for example. NFC enables bi-directional communication through dual-mode hardware, so a device can act as both a reader and a tag. For example, you can "bump" two Android phones together and exchange information using the NFC standard, or set up a secure session to exchange crypto for payment.

NFC allows communication from passive tags. For example, when you place your NFC-enabled credit card on a tap-to-pay credit card terminal, the energy from the NFC reader sends a burst of energy and excites the NFC chip in the card. At the same time the reader is verifying the card, the card is ensuring that the reader is valid. This kind of two-way processing isn't something you can do with passive RFID; when the passive reader sends out a burst of energy, the passive RFID tag can only transmit back a number.

Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of communicating, monitoring, detecting, and controlling.**

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be equipped with a radio frequency (RF) chip for the locking, disabling a lock, enabling a lock, and unlocking the locks of containers, vehicles, houses and businesses, and are capable of a two-way, bi-directional radio frequency (RF) communication link that makes the cell phone, the smart phone, and the cell

phone detector case work as a radio frequency (RF) sensors or a radio frequency (RF) transceiver.

CMDC DEVICE / DETECTOR CASE

The Smartwatch has the same features as the cellphone detector case and the CMDC Device (i.e. smartphone) described in the Patents owned by Larry Golden.

C – Communicating: cellular, Bluetooth, Wi-Fi, GPS, NFC, E-mail, call alerts, alarms
M – Monitoring: heart rate monitor, blood pressure monitor (i.e. chem/bio monitoring)
D – Detecting: carbon monoxide, natural gas, blood oxygen, seizure (i.e. chem/bio detection)
C – Controlling: lock and unlock doors, remote vehicle controls to include engine start

Patent Claim The multi-sensor detection system of claim 81, wherein the multi sensor detector device is a multi-sensor embedded or built-in device designed for, but not limited to, at least one of a cell phone, a smart phone, a PDA, a handheld, a cell phone detector case, a smart phone detector case, a PDA case, a handheld case or another communication device.

Patent Claim The multi-sensor detection system of claim 103 wherein each cell phone detector case includes an internet connection, a GPS connection, a radio frequency (RF) connection, a recharging cradle or seat, a front side, a top, a bottom, a pair of opposed sides and a central processing unit (cpu).

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone; the smart phone; and the cell phone detector case includes standard keypad functions and more specialized system use ring tone, email, photos, and texting functions as well as viewing screens.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case includes telecommunication, telematics, long and short range radio frequency communication means that are interactive with any type of motive vehicle comprising a car, truck, van, SUV, train, subway, boat, ship, UAV, UGV, or airplane.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone the smart phone, and the cell phone detector case are capable of sending signals to a vehicle's operating equipment systems comprising at least one of an ignition for starting and stopping, a lock for unlocking and locking, a horn for sounding; and are capable of receiving data and diagnostic information of the vehicle's operating equipment systems.

“WHO” INVENTED THE SMARTPHONE?

BY LARRY GOLDEN

BROAD AGENCY ANNOUCEMENT (BAA)

BAA07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Published: ***10/30/2007***
BAA07-10
Published: **10/30/2007**

INTRODUCTION

This solicitation is a Broad Agency Announcement (BAA), as contemplated in Federal Acquisition Regulations (FAR) 6.102(d)(2) and 35.016. A formal Request for Proposal (RFP) will not be issued in this matter.

The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate will not issue paper copies of this announcement. DHS S&T reserves the right to select for award and to fund all, some, or none of the full proposals received in response to this solicitation. No funding for direct reimbursement of proposal development costs will be allowed. Technical and cost proposals, or any other material, submitted in response to this BAA will not be returned.

However, depending on the markings on the proposal, DHS S&T will adhere to FAR policy on handling source selection information and proprietary proposals. It is the policy of DHS S&T to treat all proposals as sensitive competitive information, and to disclose their contents only for the purpose of evaluation.

Awards may take the form of contracts or other transactions agreements (OTAs). In the event an offeror or subcontractor is a Federally Funded Research and Development Center (FFRDC), Department of Energy National Laboratory, or other Federally funded entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 U.S.C. 1531) or other appropriate authority.

Depending on the nature of the full proposals received, DHS S&T will also consider awarding a grant or cooperative agreement. Therefore, the applicable laws and regulations governing the legal vehicle used for award will depend on the legal vehicle chosen by DHS S&T. In this regard, offerors should propose a preferred vehicle type for DHS S&T to consider for award.

I. GENERAL INFORMATION

1. Agency Name

Department of Homeland Security
Science & Technology Directorate
Washington, DC 20528

2. Research Opportunity Title

Ubiquitous Biological and Chemical Sensing

3. Program Name

CELL-ALL

4. Research Opportunity Number: BAA07-10

5. Important Dates

Event Date Time (local Eastern Time)

White Paper Due Date **11/29/2007** 4:30 P.M.
Notification of Evaluation of White Papers 12/14/2007 N/A
Full Proposal Due Date **01/14/2008** 4:30 P.M.

(A Full Proposal will not be accepted unless a White Paper was received before the White Paper due date specified herein AND the Offeror was encouraged to submit a Full Proposal.)

Notification of Evaluation of Full Proposals/Recommendation for Award 02/08/2008 N/A
* There is a registration process (see Section 4 of this BAA). A Prospective Offeror must ensure that it allow itself sufficient time to complete the registration and submission process. Extensions will NOT be granted.

Oral Presentations – Prospective Offerors are NOT provided the opportunity to make oral presentations.

6. Research Opportunity Description -

DHS S&T has designated this program as a High Impact Technology Solution (HITS), which is designed to a provide proof-of-concept answers within one to three years that could result in high-payoff technology (revolutionary) breakthrough. DHS S&T is seeking out those innovative, "out-of-box", possibly disruptive technologies (disrupting the normal evolutionary technological development process). It is recognized that this project will have considerable technological risk; however it also offers the potential for significant gains in capability.

Innovation is critical. Offerors should demonstrate that their efforts are aimed at high-risk/high-payoff technologies that have the potential for making revolutionary rather than incremental improvements to homeland security, including emerging threats and operational challenges. ***DHS S&T reserves the right to select for award and fund all, some, or none of the Full Proposals received in response to this solicitation.***

Today's biological and chemical sensing networks work effectively to cover limited and specific physical areas and environments with significant cost and overhead. In order to greatly expand coverage and realize greater WMD protection for the nation, a revolutionary breakthrough that provides for a much larger and lower cost sensing distributed network is required. For example, if biological and chemical sensors could be effectively integrated into common cell phone devices and made available to the American public on a voluntary basis, the Nation could potentially benefit from a sensor network with more than 240M sensors. Through this BAA, HSARPA is seeking to accelerate advances in miniaturized biological and chemical sensing (e.g. laboratories on a chip) with integration into common device(s) and a communication systems concept for large scale multi-sensor networks. This proof of concept should be capable of detecting hazardous biological and/or chemical materials with eventual expansion to the detection of explosive and eventually radiological materials (in future collaborations with other organizations). In the first year, proposed work should lead to a minimum of a relevant laboratory demonstration of a proof of concept sensor, device and communications system for Cell-All. Optional second year work may be proposed to build upon success in year one and may include additional field experiments and characterizations.

The proposed concept should develop a miniaturized sensor, device and system that when integrated is capable of addressing the following performance characteristics:

• Integrated into a common domestic platform, such as a cell phone
• User enabled so that the device can be switched on or off at the discretion of an individual user.
• Low cost and easy to maintain at scale
• Capable of accurately and securely communicating the location, date, time and binary outcome of sample readings
• Capable of receiving and displaying warning information from operations centers
• Demonstrates significant potential to provide accurate readings in a wide variety of environments
• Provides adequate sample collection methods within the host device to enable accurate sensing
• Provides sensing capability for multiple samples and any required methodology to readily refresh consumables
• Provides a reasonable power profile that does not significantly degrade the performance of the host device
• Survives a variety of environmental conditions
• Demonstrates an effective lifetime of more than one year.
• Supported by developmental architectures and development environments that promote low cost experiments, spiral prototyping and wide scale implementation

The contractor will also:

• Clearly define risks and vulnerabilities of the recommended technical approach and address methods to mitigate those risks and vulnerabilities
• Identify any barriers to ubiquitous sensing using the collection and sensor devices as proposed
• Provide a rough order of magnitude estimate of costs and overall schedule to develop each component and integrate into an overall system.
• List relevant experience in efforts that are similar

DHS S&T is receptive to individual or team offers. Technology developers must describe the schedule of incremental products they expect to produce.

7. Government Representatives

Science and Technology
Stephen Dennis, Program Manager
Department of Homeland Security
Science and Technology (S&T) Directorate
Washington DC, 20528

Business
Margaret L. "Margo" Graves
Team Lead/Contracting Officer
Department of Homeland Security
Office of Procurement Operations/

"Proposal White Paper"

BROAD AGENCY ANNOUNCEMENT (BAA) 07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Administrative and Technical Points of Contact:

Larry Golden, CEO
ATPG Technology, LLC
522 Peach Grove Place
Mauldin, SC 29662
864-288-5605 / 864-992-7104
Lgolden5605@charter.net

Executive Summary:

Two years ago, recognizing the danger that existed if a WMD was concealed, transported and deployed within our borders, ATPG embarked on the development of a multi-sensor, tracking and detection system. The first development spiral yielded a functional Sensor Monitoring Device (SMD) prototype and tiered communication applications to distribute, monitor and manage the multi-sensor SMD network information. The ubiquitous sensor network solution proposed in this white paper borrows heavily from the technology developed in spiral one. The tiered communication, viewer and management software applications were designed to be part of a large sensor network. For this application the software will be scaled and enhanced to accommodate the volume of traffic that would result from an extremely large sensor network.

Our SMD was designed to provide as much flexibility as possible and communicates with a variety of sensors through an array of built-in standard interfaces (SPI, A/D, Serial, Bluetooth, I2C etc). This existing open architecture design affords us the opportunity to collaborate with the U.S. Army Edgewood Chemical and Biological Center (ECBC) to evaluate, test and acquire the most appropriate miniaturized chemical and biological sensors.

ATPG intends to utilize the hardware and software technology developed in spiral one as the basis for the ubiquitous sensor network. The form factor of the SMD will be re-engineered so that it can initially be housed in cell phone cases allowing straightforward integration with existing cell phones. The SMD, housed in the cell phone cases will use a Bluetooth channel to communicate with ATPG software hosted on the cell phone. This software will provide bidirectional communication between the SMD and cell phone. The cell phone software will additionally use email and SMS messaging services to communicate information to control centers. The software for managing the information from the sensor network will be architected in a way that provides a means to efficiently escalate information up the government hierarchy.

The software will employ a large database back-end and where practical message routing rules will be implemented to allow for effective and efficient routing of sensor message traffic.

Utility to Department of Homeland Security:

ATPG's strategy of incorporating its existing SMD design into cell phone cases provides a means to quickly establish a massive sensor network nationwide. ATPG proposes modifying the SMD form factor so that it can be installed into the most common cell phone cases. When a person volunteers for the program they would receive a cell phone case along with an adapter

cord that would connect to their existing phone charger; allowing the SMD and phone to charge simultaneously. A switch on the case will allow the volunteer to enable the device at their discretion. If a volunteer elects to participate in the program and their cell phone does not have an on board GPS, the SMD provided in the cell phone case will be equipped with one. The geographic position of the SMD/cell phone pair will be determined either by GPS, cell phone tower database and signal strength or by a Wi-Fi hotspot database. In the event current position cannot be determined, the device will use its last known good position fix for communications and the position will be flagged as such. Housing the SMD and sensors in a cell phone case provides a number of advantages. Since the SMD will draw all of its power from its own power source the only resources required from the cell phone will be for a dedicated Bluetooth channel and limited processing power to execute the cell phone software. Additionally the consumables in the cell phone case (battery, sensors etc.) can easily be switched out, or the entire case can be easily replaced. ATPG will be working with the Otter Box Company to design a cell phone case capable of housing the SMD and its sensors, providing a protective, water resistant case while maintaining complete cell phone interactivity. This approach will allow ATPG to easily and incrementally make changes to the host platform as the technology of the SMD and its sensors are miniaturized.

Technical Approach:

The creation, implementation and management of a massive sensor network will require a design approach that delivers a system solution. Every tier of the system is important and the end product must be manageable, provide redundancy and implement an open architecture wherever possible. The ATPG solution proposed here focuses on these requirements and delivers a design that translates into a straightforward, deployable sensor network system that can be distributed en masse.

At the lowest level, the SMD is engineered to communicate with a variety of sensors through an array of standard interfaces (SPI, A/D, Serial, I2C etc). This open architecture allows for easily integrating additional sensors into the device and expanding the range of hazardous agents detectable by the SMD. The SMD will continually monitor/control the attached sensors and communicate with the cell phone via a dedicated Bluetooth channel. When the SMD is activated by the user, a small software application installed on the phone will monitors the

Bluetooth channel for detection alerts and also forward commands received from control centers to the SMD. The SMD will periodically send its position information to the control center. The position the SMD will report to the control centers is determined using a layered approach.

Initially the SMD will look to the on-board GPS (if provided) to determine position. If the cell phone is equipped with a GPS the application on the cell phone will retrieve the position from its own GPS. When a GPS position cannot be determined, the position of the SMD and its user will be calculated based on a cell phone tower database, provided by the FCC and signal strength. If this does not yield a result, the Wi-Fi hotspot database will be utilized to determine SMD and user position. If all these options fail, the last known position can be augmented with the on board accelerometers to estimate the current position which will be reported to the control centers and annotated as a last position and a possible position. All information received by the cell phone application from the SMD will be forwarded to the control centers either through email or SMS messages if email is not available. The information transmitted will be encoded in XML and encrypted prior to transmission. When a user needs to be notified of information from a control center, the cell phone software will use either a ring tone or vibration to call the user's attention to the display. This solution of integrating the SMD into the cell phone case and installing a small software application on the volunteer's cell phone provides a means to easily modify and upgrade the sensor network system as advancements are made to sensor and SMD technology with minimal impact to the user.

The web and desktop software that support the sensor network is designed to support an escalating reporting hierarchy. At each level rules can be established in the message routing software to facilitate the transfer of alert information. Rules can also be established to assist in determining the area affected by an alert. In the event a chemical or biological agent is detected and reported, the software can automatically search for other sensors in a pre-defined area and command them to sample and report back. This information can then be used by first responders and local government to determine the impacted area and aid in creating a plan of action to cope with the event. The reporting hierarchy can be configured as needed but the current configuration sends notification to the local First Responder units, followed by City, County, State and Federal government. As the information works its way up the hierarchy rules at each level fire off to create events that notify necessary personnel at each level. The viewer/management software used at each level of the hierarchy is identical. How the system forwards and responds to data is

configured in the message routing rules table. The desktop software uses Google Earth as a viewer and plots the position of the sensors and detections on the map. Filtering options are provided in the software to allow the screen to be decluttered. A hierarchical database of sensors reporting to the viewers at a given control center is maintained to allow simple manipulation of the sensor network. The software will allow the user to drill down into lower levels of the data by clicking on the images on the map or through the windows explorer like interface provided.

The software will also allow commands and alerts to be sent to SMD enabled cell phones by clicking on the image or on its text representation. Each SMD representation on the map will display its unique identification number as its label and clicking on the icon will display the last set of data received by the control center. The sensor network data can also be made available to smart phones and PDAs running a variation of the viewer/management software. All data passed through this network will be encrypted and all database and user accounts will be protected by multiple layers of security to ensure the privacy of the volunteers and protect their location from foreign/unwanted access.

As an option all messages sent from the SMD to the control centers could receive notification of receipt; confirmation that the network is operating properly. This could be a built-in fail safe, which would allow the user to be notified first if detection occurred and the information could not be transmitted to a control center. In this scenario the user would be notified of the detection and could take action to leave the area and contact authorities through some other means.

Personnel and Performer Qualifications and Experience:

Larry Golden is the CEO of ATPG and will be the project manager for this program. Mr. Golden's invention and patent pending sensor monitoring device (Pub. 10-18-07; App. #: 11/397,118) will be used as the departure point for the development of the SMD. Mr. Golden's background is in industrial engineering and management. Larry's duties will include managing the schedule, budget and subcontractors providing the cell phone cases.

Harold Kimball is a software engineer with twenty years' experience developing software applications, including embedded systems, operational flight programs, database applications, and web and desktop applications. Mr. Kimball will be the technical lead on this program as well as the lead software developer for the SMD applications. Over the past few years Mr. Kimball's focus has been on developing situational awareness applications, embedded device applications

and aircraft simulation software. Mr. Kimball has a Bachelor's degree in Computer Science and is working on his Master's Degree in Artificial Life. Mr. Kimball recently had an article published describing a scalable disaster relief and communications infrastructure system he is developing to aid first responders and disaster relief personnel in their efforts.

Doug Cumbie is an electrical engineer and software engineer with six years' experience developing embedded systems, web applications, situational awareness software and aircraft simulation software. Mr. Cumbie will be the lead Engineer on this program as well as the primary developer for the web and desktop applications. Over the past few years Mr. Cumbie has focused on embedded device development, situational awareness applications and aircraft simulation software. Mr. Cumbie holds Bachelor's degrees in both Computer Engineering and Electrical Engineering.

The Otter Box Corporation will provide custom cell phone cases for housing the SMD developed by ATPG. The Otter Box Corporation has extensive experience manufacturing and distributing custom cases for cell phones, laptops and PDAs. Their manufacture and distribution experience will play a key role in the ability to efficiently develop, manufacture and distribute a custom cell phone case enveloping the SMD and providing a water resistant and protective case. U.S. Army Edgewood Chemical and Biological Center (ECBC) will play a vital role in assisting ATPG with evaluating, testing and selecting the most appropriate miniaturized chemical and biological sensors available. ATPG and ECBC have a collaborative agreement in place ensuring ATPG of their services in sensor analysis and selection.

Commercialization and Capabilities:

ATPG will work closely with Otter Box and ECBC to determine the physical characteristics and requirements needed to create a custom cell phone enclosure for the selected sensors and SMD. ATPG will leverage Otter Box's manufacturing and distribution experience to enable ATPG to produce and deliver large quantities of custom cell phone cases. As mentioned previously the case will be designed and developed so that consumables can easily be swapped out or the entire cell phone case can be replaced. This approach ATPG is pursuing is the most economical and efficient way to mass distribute a sensor network; providing low risk and minimal impact to volunteers of the program. Becoming part of this volunteer network would be a simple process and would only require end-users to; elect to become a volunteer, indicate which type of cell phone they currently use and upon receipt of the new cell phone case

commence holstering the cell phone in the case wherever they go. As an option and to solicit interest in the program, volunteers could be provided software applications. These applications could potentially access tracking information of the volunteer's phone and the volunteer's family members' phones; or a moving map application could be provided to enable navigation through the cell phone. Mr. Kimball and Mr. Cumbie have many years' experience developing and distributing code to demanding end users. Both individuals have experience providing Situational Awareness and OFP software to the Air Force Special Operations Command (AFSOC) for all fixed wing Special Operations Forces (SOF) aircraft. Additionally, Mr. Kimball worked for Manheim Auctions, an international organization with a large customer base and participated in the development and distribution of Manheim's software applications.

One method ATPG conceived for fielding the sensor network and implementing its widespread use would be to conduct a pilot program for the nearly 30 million government employees, border patrol personnel and government contractors. These individuals generally work in what would be considered high value target areas. Providing these employees with cell phone cases equipped with the SMD and its sensors would immediately give the sensor network nationwide coverage in many areas that would be likely targets of a terrorist attack. In addition to gaining nationwide coverage; if this pilot program extended to all government employees and its contractors around the world, the network would have the ability to monitor U.S. interests globally.

Costs, Works and Schedule:

The budgeted cost for this development is $1,000,000, with a projected period of performance of one year. ATPG will simultaneously commence four primary tasks upon contract award.

1) ATPG will work with ECBC to evaluate, test and select the most appropriate chemical and biological miniaturized sensors available (4 month effort, $17,137)).

2) ATPG will research and determine the three most commonly used phones capable of being part of this sensor network and work with Otter Box to design and manufacture cell phone cases to house the SMD and sensors (4 month effort, $45,000).

3) ATPG will enhance/scale the software applications to support the potentially large volume sensor network that will comprise the Cell-All ubiquitous system (7 month effort, $500,000).

4) ATPG will restructure and scale down the SMD so it can be accommodated in the cell phone case. After month 7, integration and testing of the Cell-All system will commence. The system will be documented (block diagrams, wiring diagrams, and theory of operation manual) and a demonstration date will be scheduled (12 month effort, $437,863).

Prototype cases housing the SMD and sensors, cell phones and viewer/management software executables will be delivered upon project completion.

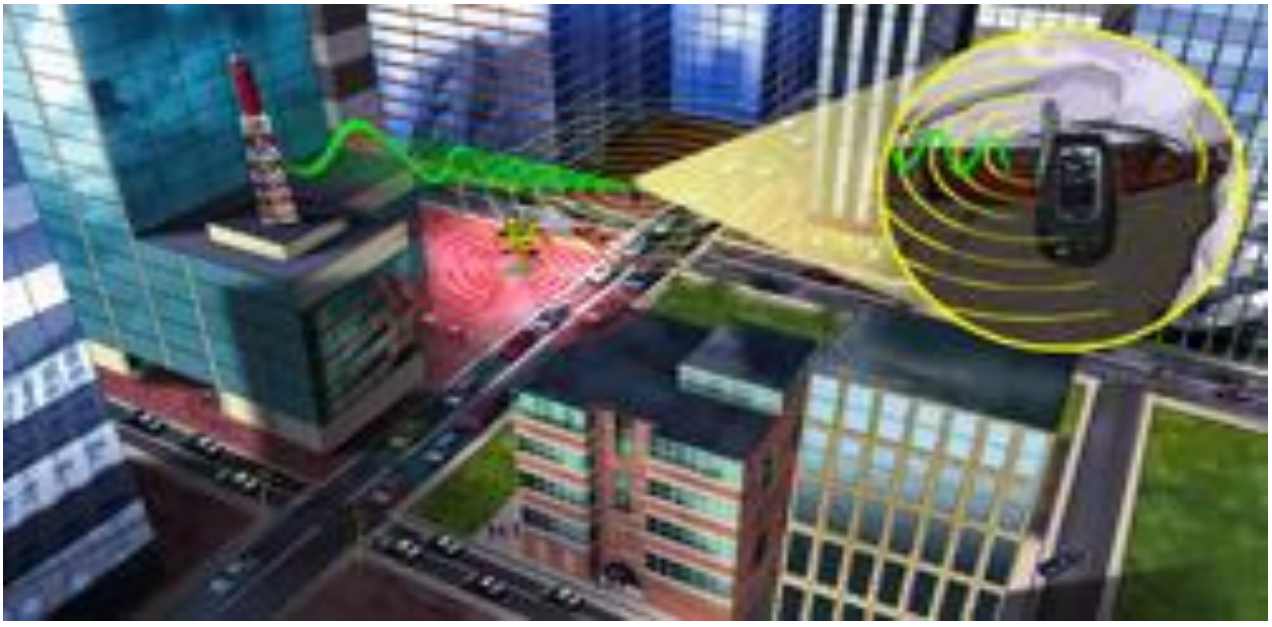
Small Business Considerations:

This white paper is submitted from a minority owned small business.

Official website of the Department of Homeland Security

2010 Archives

Cell-All: Super Smartphones Sniff out Suspicious Substances



Years ago, if you wanted to take a picture, you needed a dedicated camera. You needed to buy batteries for it, keep it charged, learn its controls, and lug it around. Today, chances are your cell phone is called a "smartphone" and came with a three-to-five megapixel lens built-in—not to mention an MP3 player, GPS, or even a bar code scanner.

This Swiss Army knife trend represents the natural progression of technology—as chips become smaller and more advanced, cell phones continue to absorb new functions. Yet, in the future, these new functions may not only make our lives easier, they could also protect us—and maybe even save our lives.

The Cell-All initiative may be one such savior. Spearheaded by the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), Cell-All aims to equip your cell phone with a sensor capable of detecting deadly chemicals at minimal cost—to the manufacturer (a buck a sensor) and to your phone's battery life. "Our goal is to create a lightweight, cost-effective, power-efficient solution," says Stephen Dennis, Cell-All's program manager.

How would this wizardry work? Just as antivirus software bides its time in the background and springs to life when it spies suspicious activity, so Cell-All regularly sniffs the surrounding air for certain volatile chemical compounds.

When a threat is sensed, a virtual *ah-choo!* ensues in one of two ways. For personal safety issues such as a chlorine gas leak, a warning is sounded; the user can choose a vibration, noise, text message, or phone call. For catastrophes such as a sarin gas attack, details—including time, location, and the compound—are phoned home to an emergency operations center.

While the first warning is beamed to individuals—a grandmother taking a siesta or a teenager hiking through the woods—the second warning works best with crowds. And that's where the genius of Cell-All lies—in crowdsourcing human safety.

Currently, if a person suspects that something is amiss, he *might* dial 9-1-1, though behavioral science tells us that it's easier to do nothing. If he does do something, it may be at a risk to his own life. And as is often the case when someone phones in an emergency, the caller may be frantic and difficult to understand, diminishing the quality of information that's relayed to first responders. An even worse scenario: the person may not even be aware of the danger, like the South Carolina woman who last year drove into a colorless, odorless, and poisonous ammonia cloud.

In contrast, anywhere a chemical threat breaks out—a mall, a bus, subway, or office—Cell-All will alert the authorities automatically. Detection, identification, and notification all take place in less than 60 seconds. Because the data are delivered digitally, Cell-All reduces the chance of human error. And by activating alerts from many people at once, Cell-All cleverly avoids the longstanding problem of false positives. The end result: emergency responders can get to the scene sooner and cover a larger area—essentially anywhere people are—casting a wider net than stationary sensors can.

But what about your privacy? Does this always-on surveillance mean that the government can track your precise whereabouts whenever it wants? To the contrary, Cell-All will operate only on an opt-in basis and will transmit data anonymously. "Privacy is as important as technology," avers Dennis. "After all, for Cell-All to succeed, people must be comfortable enough to turn it on in the first place."

For years, the idea of a handheld weapons of mass destruction detector has engaged engineers. In 2007, S&T called upon the private sector to develop concepts of operations. Today, thanks to increasingly successful prototype demonstrations, the Directorate is actively funding the next step in R&D—a proof of principle—to see if the concept is workable.

To this end, three teams from Qualcomm, the National Aeronautics and Space Administration (NASA), and Rhevision Technology are perfecting their specific area of expertise. Qualcomm engineers specialize in miniaturization and know how to shepherd a product to market. Scientists from the Center for Nanotechnology at NASA's Ames Research Center have experience with chemical sensing on low-powered platforms, such as the International Space Station. And technologists from Rhevision have developed an artificial nose—a piece of porous silicon that changes colors in the presence of certain molecules, which can be read spectrographically.

Patent Claim A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological

sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.

Continue from DHS official site: Similarly, S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: **Qualcomm, LG, Apple, and Samsung.** These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.

To be sure, Cell-All's commercialization may take several years. Yet the goal seems imminently achievable: Just as Bill Gates once envisioned a computer on every desk in every

home, so Stephen Dennis envisions a chemical sensor in every cell phone in every pocket, purse, or belt holster. If it's not already the case, our smartphones may soon be smarter than we are.

To request more information about this story, please e-mail st.snapshots@hq.dhs.gov.

THE GOVERNMENT ENTERED INTO AGREEMENTS WITH APPLE, SAMSUNG, LG, AND QUALCOMM FOR THE DEVELOPMENT AND COMMERCIALIZATION OF THE 'CMDC' DEVICE (i.e. Modified CELL PHONE). APPLE, SAMSUNG, LG, AND QUALCOMM's INFRINGEMENT OF THE COMMUNICATING, MONITORING, DETECTING, AND CONTROLLING (CMDC) DEVICE IS ILLUSTRATED BELOW.

"TESTING MECHANISM CLAIM CHART" TO DETERMINE INFRINGEMENT

Read from Left>>>>>>>>>>>>>>>>>>>>>>>>>>>> to >>>>>>>>>>>>>>>>>>>>>>>>>>>>Right>>>>>>>>>>

Apple's iPhone 5, 5c, 5s, 6, 6, 7, 8, 9, and 10 and the iPad interconnected to the Apple Watch	**Patent #: 9,589,439; Independent Claim 22**	**Patent #: RE 43,990; Dependent Claims**
The Apple Watch (e.g. multi-sensor detection device: interconnected to monitoring equipment – iPhone / iPad; biosensor for detecting heart rate; leveraged internet and GPS connections; power source battery; CPU; light indicators). Apple Watch requires an iPhone 5, 6, 7, 8, 9, and 10.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring

The heart rate bio-chemical sensor in Apple Watch uses photoplethysmography (heart rate (HR) and pulse oximeter oxygen saturation (SpO2) from wearable photoplethysmographic (PPG) biosensors). Technology based: Apple Watch can calculate the number of times the heart beats each minute; your heart rate.	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.
Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. The iPhone 6's A8 processor has a dual-core model like the A7, but clocked at a higher frequency. The iPhone 6 has a 2GHz dual-core 20nm 64-bit A8 CPU.	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).
If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Every iPhone and iPad ever made has both WiFi and Bluetooth. The cellular service, originally called 3G and now called LTE; allows the iPhone to connect to the internet anywhere cell phone works. The iPhone uses the GPS chip in conjunction with cell phone towers and Wi-Fi networks—in a process termed "assisted GPS".	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). iPhone and iPad Touch ID use fingerprint as a passcode. Fingerprint one of best passcodes in the world. With just a touch of the device's Home button, the Touch ID sensor quickly reads a fingerprint and automatically unlocks the phone.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...

If Apple Touch ID doesn't recognize your finger after multiple failed attempts, you'll be given the option of entering your Apple ID password. You need to enter your Apple ID password after: (1) Restarting your device, and (2) Enrolling or deleting fingers. If lost or stolen, you can disable Touch ID from being used to unlock your device with Find My iPhone Lost Mode. Additional protection against theft with Activation Lock,	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
iPhone and iPad Touch ID is a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...
NFC arrived on the iPhone 6 in 2014, it has been restricted to the contactless Apple Pay system. But at the Worldwide Developers Conference last week, Apple quietly announced that with the arrival of iOS 11 this fall, apps will be able to use an iPhone’s NFC chip to read tags, pair with accessories, and exchange data with other NFC devices.	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.

Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails. The iPhone's GPS chip is like that found in stand-alone GPS devices. The iPhone uses the GPS chip in conjunction with cell phone towers and Wi-Fi networks—in a process termed "assisted GPS"—to quickly calculate the phone's position.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails. Apple chip A8X delivers better CPU and graphics performance than its predecessor. The iPhone 6's A8 processor has a dual-core model like the A7. The iPhone 6 has a 2GHz dual-core 20nm 64-bit A8 CPU.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

Samsung Galaxy s6 interconnected to the "Samsung Gear S2 Smartwatch"	Patent #: 9,589,439; Independent Claim 22	Patent #: RE 43,990; Dependent Claims
The Samsung Gear S2 smartwatch (e.g. multi-sensor detection device: interconnected to monitoring equipment – Samsung Galaxy s6; biosensor for detecting heart rate; leveraged internet and GPS connections; power source battery) has a solid health tracking and slightly better battery life than other high-end smartwatches. It works with a variety of Android phones.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring
The Gear S2 need to connect to a mobile device (e.g. Galaxy S6) using the Samsung Gear application. The application must be installed on the mobile device (e.g. Galaxy S6). The Gear S2 sensors include: Accelerometer; Gyroscope; Heart Rate; Ambient Light; and, Barometer. Connectivity include: 802.11n WiFi; Bluetooth 4.1; NFC. GPS include: The Gear S2 3G includes a GPS receiver and two apps, Nike+ and S Health, that include GPS tracking support.	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.

Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. The Samsung Galaxy S6 SM-G920i 32GB is a good Android phone with 2100 MHz processor 8-core that allows the user run heavy applications. The Samsung Galaxy S6 smartphones and tables don't just use "processors", they use what's called a System-on-a-chip (SoC). The SoC is the equivalent of a computer motherboard, including main processor, graphics processor and memory, on a single chip. The CPU is nonetheless a must-have component of the SoC. Modern SoCs have two, and soon four, processors cores ("multi-core")	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).
The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 "Fingertip Heart Rate Monitor" detection device (e.g. cell phone detection device) is a built-in monitor that measures heart rate from a fingertip using a biosensor.	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

The Samsung Galaxy S6 capable of receiving a signal to reset (e.g. unlock; locking device) the phone. The Samsung Galaxy S6 "Fingertip Heart Rate Monitor" detection device (e.g. cell phone detection device) is a built-in monitor that measures heart rate from a fingertip using a biosensor.	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Cellular data connection: The connection that the Galaxy s6 uses to exchange data over the air using your mobile operator's cellular network. Cellular network connection: the Galaxy s6 uses for voice and data connect. This network is managed by the mobile operator.WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP, LE,	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Seven wireless interfaces in the Samsung Galaxy S6 smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging. Samsung allows 4 fingerprints to set-up the fingerprint scanner; for log-in and lock-out. Samsung's Face unlock uses the front-facing camera to identify the user and unlock the device. Samsung's iris scanning method, uses special sensors on front of phone to identify and unlock the device.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If user is unable to log in after doing all the security layers, there's no other option but to have the phone unlocked. Samsung's near-field communication (NFC) enabled smartphone: slide hand on the back and the NFC Ring can unlock it. The NFC Ring comes with two special NFC tag inlays inside the ring. The NFC Ring can be used to unlock & control mobile devices	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out. Samsung's new Face unlock feature uses the front-facing camera to identify the user and unlock the device. Samsung has included an iris scanning method, which uses special sensors on the front of the phone to identify you and unlock the device. Iris scanning is considered one of the most secure biometric methods	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.
Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.

Cellular data connection: The connection that the Galaxy s6 uses to exchange data over the air using your mobile operator's cellular network. Cellular network connection: The network that the Galaxy s6 uses for making voice and data connections. This network is managed by the mobile operator.WLAN: Wi-Fi 802.11, Wi-Fi Direct, and hotspot. Bluetooth: v4.1, A2DP, LE, apt-X. The Galaxy can determine location using its built-in Global Positioning System (GPS) transmitter, Wi-Fi networks, and mobile networks.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 capable of receiving a signal to reset (e.g. unlock; locking device). Thereby activating or deactivating a security system.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

LG Electronics: LG V10 Smartphone; LG Watch Sport	Patent #: 9,589,439; Independent Claim 22	Patent #: RE 43,990; Dependent Claims
2008: The "Cell-All" initiative. The DHS-S&T, Cell-All aims "to equip your cell phone with a sensor capable of detecting deadly chemicals", says Stephen Dennis, Cell-All's program manager. S&T pursued cooperative agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. Used by the Government; 2016: Both the LG G5 and V10 smartphones is used by the Department of Defense. Sensors will integrate with 261 million cell phones.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring
The LG Watch Sport is, well, sporty-looking with a big 1.38-inch, 480-by-480 P-OLED display. The device has two buttons for convenient navigation and integrates multiple sensors, including an accelerometer, barometer, ambient light, GPS, and a PPM sensor (short for photoplethysmogram, which accurately tracks heart rate when the wearer is at rest or active).	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.
LG V10 CPU: Hexa-core (4x1.4 GHz Cortex-A53 & 2x1.8 GHz Cortex-A57). LG smartphones are equipped with embedded chipsets. The CPU that's at the core of the chipset is vital for general computing performance. LG V10 Chipset: Qualcomm MSM8992 Snapdragon 808	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).

Transmits signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. You can use Bluetooth to transfer information between LG V10 phone and another Bluetooth-enabled device. Quick message is the specified text message to send out.	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Receives signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. LG V10 User Guide: Notifications: Enable this option if you wish to receive a notification when a new text or multimedia message arrives.	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
LG V10 cellular connection; Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot; Bluetooth 4.1, A2DP, LE, aptX ; GPS with A-GPS, and GLONASS	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

LG V10 features include sensors for face/smile detection, iris scanner, and fingerprint recognition.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...
After 5 unsuccessful attempts to unlock the LG smartphone, the user is prompted to enter a text phrase to confirm that they are trying to unlock the phone. After 10 unsuccessful attempts, the phone will automatically perform a factory data reset and all of the personal files will be erased.	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
LG V10 features include sensors for face/smile detection, iris scanner, and fingerprint identification.	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...

The LG V10 NFC is a short-range high frequency wireless communication technology that enables the exchange of data between devices over about a 10 cm distance. It allows users to share content between digital devices, and even use their LG smartphone on existing contactless infrastructure. The significant advantage of NFC over Bluetooth is the shorter set-up time (under a 1/10 second).	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.
LG V10 cellular connection; Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot; Bluetooth 4.1, A2DP, LE, aptX; GPS with A-GPS, and GLONASS. Smartphone manufacturers and operators have introduced the Assisted GPS technology, which downloads the current ephemeris for a few days ahead via the wireless networks and helps triangulate the general user's position with the cell towers thus allowing the GPS receiver to get a faster lock at the expense of several (kilo) bytes.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

Transmits and receives signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. You can use Bluetooth to transfer information between LG V10 phone and another Bluetooth-enabled device. Quick message is the specified text message to send out. LG V10 User Guide: Notifications: Enable this option if you wish to receive a notification when a new text or multimedia message arrives.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

ITC Provides Clarity on the Meaning of a Section 337(a)(2) "Article"

ITC Provides Clarity on the Meaning of a Section 337(a)(2) "Article"

A recent decision by the International Trade Commission ("ITC" or the "Commission") held that pre-commercial or non-commercial items qualify as "articles" for purposes of section 337 investigations.[1]The decision opens up the ITC to complainants who are in an earlier phase of product development. Under section 337(a)(2), a Complainant bears the burden to show that the "domestic industry requirement" is satisfied by showing that an industry in "*articles* protected by the patent, copyright, trademark, mask work, or design concerned, exists or is in the process of being established."[2] The question that remained was whether the protected article had to be in production. In its 1046 Investigation opinion, the Commission has provided some much-needed clarity.[3] In reversing the Initial Determination, the Commission held that Section 337(a)(2) "does not require commercial production for a domestic industry in the process of being established."[4]

In the 1046 Investigation, Complainant Macronix asserted that a domestic industry in the process of being established existed based on its research and development on an experimental semiconductor wafer as its "article."[5] While the Macronix product was not a commercial product at the time of filing the complaint, or the hearing, Macronix argued that the domestic industry requirement does not require showing that the domestic industry article is a mass-produced or commercialized product.[6] The Macronix product was not ready for the marketplace, but a small quantity of precursors were made for the purpose of further research and development, and, Macronix argued, the product practices the asserted patents.[7]

In the Initial Determination, ALJ Lord agreed with Respondent Toshiba, and held that while Section 337 allows for complainants seeking to protect "nascent industries" to prevail by showing a domestic industry "in the process of being established," the statute nevertheless requires a showing of an "article of commerce, *i.e.*, a product for sale in the marketplace" to satisfy the "article" requirement of the Section 337(a)(2) domestic industry requirement.[8] Thus, ALJ Lord held that within the provisions and purpose of Section 337(a)(2), "article" refers to "products or other commodities that are sold in the marketplace."[9] According to the ID, Macronix's product was not "commercially viable" and, therefore, Macronix did not satisfy the domestic industry requirement, and no exclusion order should issue.

After both sides and the OUII Commission Staff appealed to the Commission, the Commission reversed the ID and issued a limited exclusion order against Respondent Toshiba.[10] The Commission disagreed with the ALJ's interpretation of "article" under section 337(a)(2), and stated that commercialization is *not* a prerequisite for proving a domestic industry based on an industry in the process of being established, and that a domestic industry may be based on a product still in the pre-commercial or non-commercial stage.[11]

The Commission explained that the term "article" is "sufficiently capacious to embrace pre-commercial or non-commercial items."[12] The holding cites a previous Commission opinion which cautioned against an interpretation of "article" that "would offer no relief to an inventor-complainant … before the complainant has had an opportunity to engage in production-oriented efforts."[13] The Commission also relied on the legislative history of Section 337 to support its holding that an "article" need not be commercialized. Using Section 337(a)(3)(C) as an example that permits a domestic industry based on licensing activities, the Commission stated

that Congress clearly intended to provide a remedy to nascent industries such as universities, inventors, and start-ups in the absence of a commercialized product where those industries would use licensing to raise the funds needed to manufacture a product.[14]

While the two-part test[15] for proving a domestic industry *in the process of being established* remains a difficult evidentiary threshold, this Commission opinion affords complainants security in initiating an investigation to thwart a "speedy infringer" where a complainant does not yet have a commercially ready product. In other words, it is now possible for complainants to go to the ITC earlier in their development cycle. Under this Commission opinion, the ITC is now an even more favorable venue for complainants in industries with lengthy research and development timelines, such as the medical device and pharmaceutical industries; or industries with rapid product updates, such as consumer electronics.

Endnotes

---

[1] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 41 (Oct. 26, 2018).

[2] 19 U.S. Code § 1337(a)(2).

[3] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 39-44 (Oct. 26, 2018).

[4] *Id*. at 41.

[5] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, ID at 142-44 (Apr. 27, 2018).

[6] *Id*.

[7] *Id*. at 150-54.

[8] *Id*. at 144-50.

[9] *Id*.

[10] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 71 (Oct. 26, 2018).

[11] *Id*. at 41.

[12] *Id*.

[13] *Id*. at 41-42 (citing *Certain Computers and Computer Peripheral Devices, and Components Thereof and Products Containing Same*, Inv. No. 337-TA-841, Comm'n Op. at 37 (Jan. 9, 2014) (rejecting the notion that the "article protected by the patent" "must be a product that came to market, or is expected to come to market, under the protective umbrella of the asserted patent that the product commercializes.")

[14] *Id*. at 42-43 (citing 133 Cong. Rec. S. 1794 (Feb. 4, 1987)).

[15] The two-part test for proving a domestic industry in the process of being established requires showing (1) "the necessary tangible steps to establish an industry in the United States" and (2) whether there is a "significant likelihood that the industry requirement will be satisfied in the future." *See Stringed Instruments*, Inv. No. 337-TA-586, Comm'n Op. at 13).

Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
12. The communication device of [claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
16. The communication device of [claim 11] wherein the communication device can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to the central processing unit (cpu).	NFC **Wireless Networking Technology Industry**	NFC chips might also be widely used in the Internet of Things. Qualcomm recently announced that it will include NXP's near-field communication (NFC) solution in the Snapdragon processor platform that powers mobile devices (e.g. smartphones), wearables (e.g. smartwatches), and automobiles

21. The communication device of [claim 11] wherein the communication device includes a power connection that is interconnected to the central processing unit (cpu) and power source can be battery, electrical, or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
22. The communication device of [claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.	Home and Community **Wireless Networking Technology Industry**	Every time you call, navigate, download, store something or talk, you've got the power of Qualcomm technology to thank. Also the advancements for your car, home and community are made possible by the mobile hardware, software and standards we pioneered. Qualcomm invented many of the technologies that the world's leading networks and devices run on—connecting new industries, services and experiences that are changing everything.
22. The communication device of [claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.	Disabling Lock **Locking Industry**	Qualcomm Technologies announced SafeSwitch in September of 2014. SafeSwitch is available to customers through its Qualcomm Snapdragon 810 processors. SafeSwitch technology - addresses mobile security threat with a kill switch solution is designed to allow device owners to remotely disable their devices in the event that they're lost or stolen - and then re-enable them in the event they're found. This helps to protect sensitive, personal data and to deter device theft.

30. The communication device of [claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.	Biometrics **Biometrics Industry**	Authenticating the user and the device. Beyond secure fingerprint identification, a Snapdragon 835 Mobile Platform provides a user with an extra level of safety using Camera Security—a camera-based biometric solution for iris and facial recognition engineered to help enhance mobile device security
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
30. The communication device of [claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.	Biometrics **Biometrics Industry**	Mobile transactions are safest when they are protected by a combination of user and device authentication methods. This helps data remain secure from the moment a user logs into their device. A Snapdragon 835 Mobile Platform contains the Qualcomm Haven™ security platform—a combination of hardware, software and biometrics technologies that help to make online banking and payments more secure than ever.
39. The lock disabler system of [claim 33] wherein the automatic/mechanical lock disabler detection device has a power connection which is interconnected to the central processing unit (cpu) and includes a power source of battery, electrical or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video

41. The lock disabler system of [claim 33] wherein the automatic/mechanical lock disabler detection device includes at least one of; a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are capable of being interconnected to a central processing unit (cpu) of the communication device.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon CPU uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
55. The multi-sensor detection system of [claim 33] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and software hardware to support a smartphone's GPS, camera, gesture recognition, video
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Cellular and Wireless Modem: Smartwatches **Electronic Device Industry**	Qualcomm supplied LTE modem in the Apple Watch Series 3. TechInsights found the Qualcomm MDM9635M, a Snapdragon X7 LTE modem in the 42mm sport band model A1861 with GPS + cellular. The modem was mated with a Samsung K4P1G324EH DRAM in the watch. TechInsights said the watch contains a Qualcomm PMD9645 PMIC and a WTR3925 RF transceiver. Apple and Qualcomm are embroiled in patent infringement disputes including investigations at the U.S. ITC, around baseband modems. Apple continues to use the Qualcomm parts in watches. Apple discontinue paying Qualcomm royalties while court's in progress.

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Cellular and Wireless Modem: Smartphone **Mobile Device Industry**	The iPhone X A1865 uses the Qualcomm MDM9655 Snapdragon X16 LTE modem. iPhone 8; Qualcomm Modem Model A1663; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 8 Plus; Qualcomm Modem Model A1664; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 7; Qualcomm Modem Model A1660; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. iPhone 7 Plus; Qualcomm Modem Model A1661; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. The Qualcomm MDM9625M is a modem LTE chipset found in the Apple MG9M2CL/A iPhone 6 Plus and iPhone 6.
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Wi-Fi **Wireless Networking Technology Industry**	With all the devices connecting to all the things, we knew we had to help ease overload. So we were the first to announce end-to-end commercial support for the next-generation of Wi-Fi. What does that mean? It translates into faster delivery and longer battery life for Wi-Fi devices—whether you're at home or on the go.

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
79. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.	Modems **Wireless Networking Technology Industry**	Qualcomm quote: "Some say the modem is the most important part of your smartphone. We couldn't agree more. With our wireless modem inside your smartphone, you've got years of engineering keeping you connected to your great big world. And isn't that why you bought that device in the first place?"
79. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.	LTE **Wireless Networking Technology Industry**	Everyone promises smarter/better/faster, but with LTE, we actually delivered. We invented the wireless standards and fundamental technologies that mobile operators rely on to meet the explosive demand in mobile data traffic. And that means you can catch up on the latest sports clips without waiting for the network to keep pace.
104. The multi-sensor detection system of [claim 103] wherein each cell phone detector case includes an internet connection, a GPS connection, a radio frequency (RF) connection, a recharging cradle or seat, a front side, a top, a bottom, a pair of opposed sides and a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
108. The multi-sensor detection system of [claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
113. The multi-sensor detection system of [claim 103] wherein the cell phone, the smart phone, and the cell phone detector case includes a power connection that is interconnected to a central processing unit (cpu), and wherein a power source can be battery, electrical, or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
126. The multi-sensor detection system of [claim 125] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Qualcomm Snapdragon Processor: Smartwatches **Industry for Processors** **Electronic Device Industry**	Samsung Gear S2 3G Watch (Qualcomm Snapdragon 400 Processor); Samsung Gear S Watch (Qualcomm Snapdragon 400 Processor); LG Watch Sport (Qualcomm Snapdragon Wear 2100 Processor); LG Watch Style (Qualcomm Snapdragon Wear 2100 Processor); LG G Watch R (Qualcomm Snapdragon 400 Processor); LG Watch Urban (Qualcomm Snapdragon 400 Processor).

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
126. The multi-sensor detection system of [claim 125] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Qualcomm Snapdragon Processor: Smartphone **Industry for Processors** **Mobile Device Industry**	Samsung Galaxy S8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy Note 8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy S7 (Qualcomm Snapdragon 820 Processor); Samsung Galaxy S5 (Qualcomm **Snapdragon 801 Processor); Sams**ung Galaxy S4 (Qualcomm Snapdragon 600 Processor); LG V30 (Qualcomm Snapdragon 835 Processor); LG G5 (Qualcomm Snapdragon 820 Processor); LG G4 (Qualcomm Snapdragon 808 Processor); LG G3 (Qualcomm Snapdragon 801 Processor); LG Pro 2 (Qualcomm Snapdragon 800 Processor).
132. The multi-sensor detection system of [claim 125] wherein the internal or external remote/electrical lock disabler includes at least one of: a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are interconnected to the central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
134. The multi-sensor detection system of [claim 125] wherein a communication device, that of a cell phone, smart phone or handheld; capable of sending signals to a vehicle's operating equipment systems of at least one of, but not limited to, an ignition for starting and stopping, a lock for unlocking and locking, a horn for sounding; capable of receiving data and diagnostic information of the vehicle's operating equipment systems.	Vehicle's Operating Systems **Automobile Industry**	Every time you navigate you've got the power of Qualcomm technology to thank. All the advancements coming to your car, home and community are made possible by the mobile hardware, software and standards we pioneered. Qualcomm invented many of the technologies that the world's leading networks and devices run on.

ONE EXAMPLE OF THE ECONOMIC STIMULUS STRATEGY IS RESTORING THE ECONOMY: APPLE – STATISTICS & FACTS

Technical innovation paired with minimalistic designs and creative advertisements, as well as the leadership of the former CEO Steve Jobs, have made Apple one of the most valuable brands in the world. The company's success translates into strong brand loyalty, as well as into an unparalleled revenue growth, from 8 billion U.S. dollars in 2004 to more than 265 billion in 2018.

The company was first founded by Steve Jobs, Steve Wozniak and Ronald Wayne in 1976 in the garage of Jobs' parents. Their first product, known as the Apple I, consisted of an assembled circuit board without many of the present-day features of a computer, such as display, keyboard or mouse. The company started to slowly grow with the development of Apple II, Apple III, Apple Lisa and the first Macintosh, launched in 1984.

After a rather uneventful period, the company resurfaced in the late 1990s with a number of strategic and technological changes: in 1997, Apple introduced the Apple Online Store, followed by the iMac and the video editing program Final Cut Pro in 1998. The iPod was launched in 2001, which marked the company's first venture away from computers and into other segments of consumer electronics. With several hundred million units sold, the iPod was a tremendous success. Its popularity however started to decline in 2008, as advanced music functions of smartphones began to substitute MP3 players. Apple's digital media store, the iTunes Store, was launched in 2003 and became one of the most popular online music stores in the world, generating several billion U.S. dollars in revenue per quarter.

In 2007, the release of the iPhone marked a revolution for the global smartphone market, due to the introduction of the first touch screen interface. In the United States especially, the iPhone has been a key product for the company, generating millions of unit sales and high levels of revenue. The iPhone is currently contributing about 60 percent to the company's total revenue. In total, Apple has sold close to 1.5 billion iPhones from 2007 to 2018 worldwide.

In January 2010, the iPad was unveiled, marking yet another milestone in the industry. The device went on to sell more than 3 million units in the first 3 months, thus setting a new benchmark in the industry. With the launch of its Apple Watch in early 2015, Apple entered the growing wearables market, competing with companies such as Samsung, Pebble and Fitbit.

As of June 2018, Apple's market capitalization reached 950 billion U.S. dollars, higher than that of competitors such as Microsoft, IBM and Google, and almost ten times more than its own capitalization in 2006. The company's market cap topped the one trillion U.S. dollars mark on 2. August, 2018, becoming the first public company worldwide to reach that milestone. After hitting a record high of 1.12 trillion in October 2018, Apple's market cap slowly dropped back to the sub-trillion level.

Apple updated its U.S. job creation web page with figures from 2016. Though Apple refreshes the site every year, this latest update coincides with CEO Tim Cook's

announcement during a CNBC interview that the company has formed a $1 billion fund to promote advanced manufacturing jobs in the U.S.

Though the fund may help the company gain favor with the current presidential administration, Apple has already been investing in U.S. hardware manufacturing for years (for example, its 2013 Mac Pros were built in Texas with U.S.-made components).

In total, Apple says it has created a total of two million jobs in the U.S. so far. In 2015 Apple spent more than $50 billion with 9,000 U.S. suppliers and manufacturers and added about 90,000 supplier and manufacturer jobs, increasing the total number to 450,000 jobs from 361,000 in 2015.

The number of people directly employed by Apple, including at its retail stores, grew from 76,000 to 80,000 in 2016.

On the software side, Apple claims that 1,530,000 U.S. jobs can be attributed to the App Store ecosystem, up from 1,400,000 in 2015. Since the App Store was launched in 2008, U.S. developers have earned $16 billion from sales, with 39 percent of that amount generated from abroad.

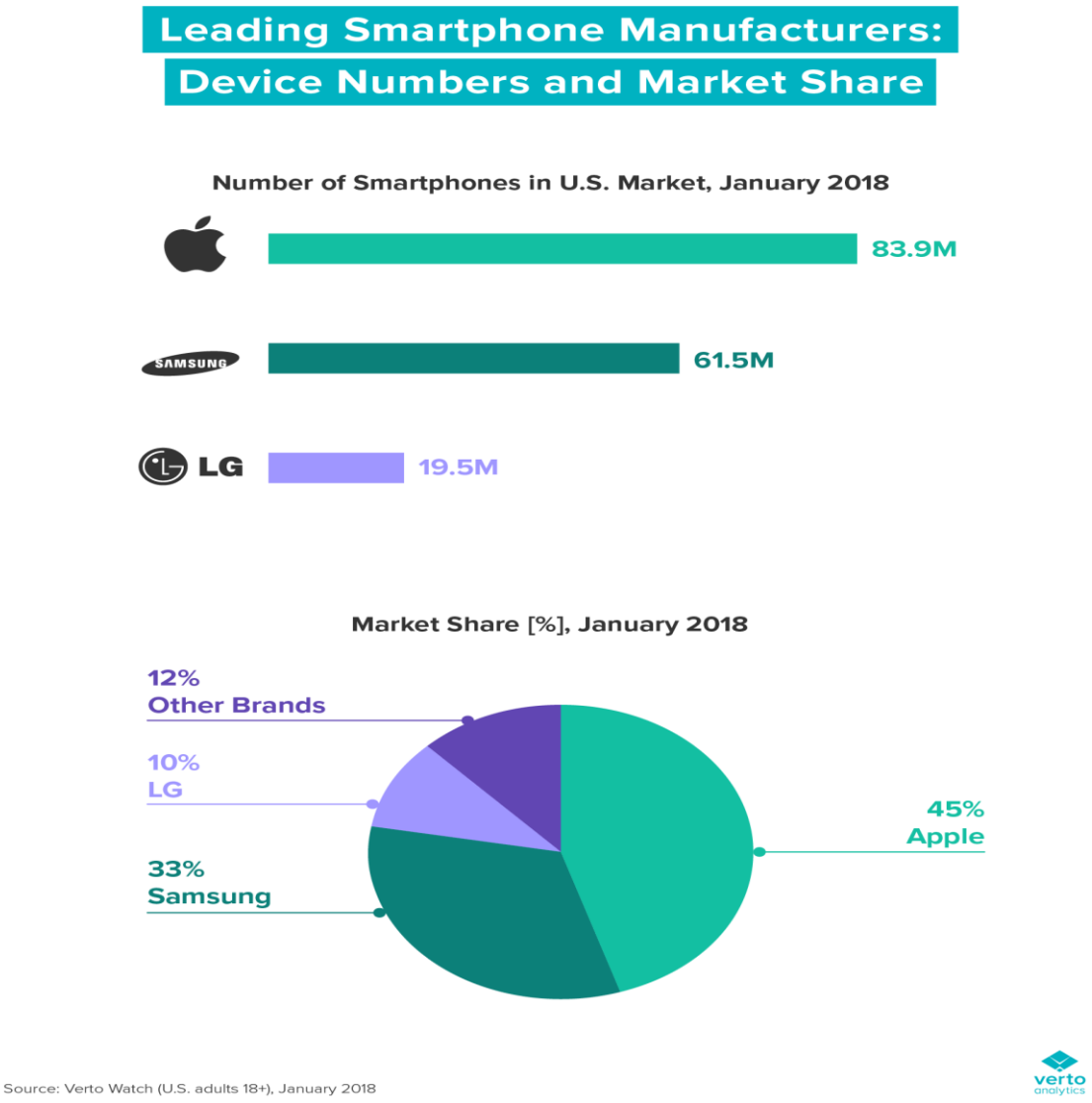
Apple also said that all of its main products (the iPhone, iPad, Mac, Apple Watch, and Apple TV) contain materials from the U.S. or are made with equipment from U.S. suppliers). It has reportedly asked its main manufacturing partners, including Foxconn, to open more factories in the U.S.

During the CNBC interview, Cook told Jim Cramer that the company will hire "thousands of employees" and is "not satisfied with just two million."

"By doing that, we can be the ripple in the pond," Cook said. "Because if we can create many manufacturing jobs around–those manufacturing jobs create more jobs around them, because you have a service industry that builds up around them."

Reference: This text provides general information. Statista assumes no liability for the information given being complete or correct. Due to varying update cycles, statistics can display more up-to-date data than referenced in the text. Image Credits: bennymarty (opens in a new window)/ Getty Images

How Do Apple, Samsung, and LG Stack Up?



Verto Analytics looked at the numbers of Apple, Samsung, and LG smartphones currently owned by U.S. consumers, and the equivalent market share. January 2018, Apple leads the pack, with 45% market share (representing nearly 84 million smartphones), while Samsung claims 33% of the market (61.5 million smartphones). These two manufacturers dominate the U.S. smartphone market; LG, the third-place contender, has 10% market share, while all other brands combined account for 12% of the devices on the U.S. smartphone market.

This Chart of the Week was created using Verto Watch.