

EXHIBIT J2 - U.S. PATENT 9,173,100 Infringement Claim Chart

Upon information and belief, all '100 Accused Instrumentalities use the same or similar structures to implement the features described in the following chart in materially the same way, unless expressly stated otherwise. Accordingly, the described structures, features, and corresponding infringement contentions are representative of infringement by all '100 Accused Instrumentalities, including Accused Instrumentalities of the Ford and Lincoln brands. In addition, the exemplary evidence cited herein, while representative of all '100 Accused Instrumentalities, is non-exhaustive and provided for illustrative purposes only. AutoConnect reserves the right to supplement or amend these contentions based on information obtained during discovery, and to rely on additional evidence consistent with the infringement theories set forth in its infringement contentions.

U.S. Patent 9,173,100		Ford Infringing Activities
Row	Claim 1	
1A	A vehicle, comprising: a plurality of on board computational components; a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and	<p>The '100 Accused Instrumentalities include a plurality of on board computational components and a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components.</p> <p>For example, the '100 Accused Instrumentalities have used several versions of the infotainment system software, including Sync 3, Sync 4, Sync 4A (the "Sync Systems"), and Ford Digital Experience ("FDE"). The Sync Systems are built on QNX platforms.¹ FDE makes use of the Android Automotive Operating System ("AAOS").² All of the '100 Accused Instrumentalities implement security mechanisms and logical perimeter networks around on board vehicle components through their in-vehicle software to enhance the safety and reliability of vehicles.</p>

¹ See, e.g., <https://techcrunch.com/2014/12/11/ford-ditches-microsoft-for-qnx-in-latest-in-vehicle-tech-platform/>; <https://www.forbes.com/sites/samabuelsamid/2019/10/30/new-ford-vehicles-to-get-sync-4-infotainment-and-ota-updates-from-2020/>.

² See, e.g., <https://built-in.google/cars/>; <https://corporate.ford.com/articles/research-and-innovation/digital-experience/>; <https://www.ford.com/technology/ford-digital-experience/>; <https://www.ford.com/support/how-tos/ford-technology/ford-digital-experience/ford-digital-experience-profile-setup/>; <https://www.nickmayerfordeast.com/blogs/6941/the-new-android-powered-infotainment-system-in-the-2025-ford-explorer-in-cleveland-heights/>; <https://www.youtube.com/watch?v=95w2mV4KJ9U>; <https://support.google.com/built-in/answer/9905854>; <https://support.google.com/assistant/answer/11091015>; <https://support.google.com/built-in/answer/13827211>; <https://support.google.com/My-Ad-Center-Help/answer/12155656>; <https://support.google.com/My-Ad-Center-Help/answer/12156161>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>For example, all '100 Accused Instrumentalities (Sync Systems and FDE) have a plurality of on board computational components, including (but not limited to) operating systems, electronic control units (“ECUs”), software domains, subsystems, and components.</p> <p>Upon information and belief, all '100 Accused Instrumentalities (Sync Systems and FDE) include a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on-board computational components. This can be done in several ways. For example, upon information and belief, the Sync Systems and FDE each use various techniques for constructing logical communication networks that include on-board computational components and enforcing security measures at the perimeter networks to protect the integrity of the system. For example, upon information and belief, the '100 Accused Instrumentalities including Sync Systems utilize firewalls, sandboxing and/or mandatory access control, and hypervisors to logically define perimeter networks around specific on-board computational components.³ Security measures are implemented at these perimeter networks by, for example, defining security policies, which control what processes are allowed and where and which processes may connect with each other. The '100 Accused Instrumentalities including FDE also use hypervisors, firewalls, sandboxing and/or mandatory access control to logically form perimeter networks around computational components and implement security policies at the perimeters.⁴</p>
1B a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,	<p>The '100 Accused Instrumentalities include a microprocessor executable network controller that can detect the instance of a breach of a security measure. For example, upon information and belief, the '100 Accused Instrumentalities include a microprocessor that runs software to enforce security policies for processes and communications at the interface of the perimeter</p>

³ See, e.g., <https://www.iotevolutionworld.com/iot/articles/456299-blackberry-qnx-software-embedded-235-million-vehicles-worldwide.htm>; <https://seeingmachines.com/wp-content/uploads/2022/10/Hansen-Report-October-2018.pdf>; <https://www.cs.bu.edu/~richwest/slides/CPS-IOTWeek-2022.pdf>; <https://www.redhat.com/en/blog/strategic-shift-how-ford-and-emirates-nbd-stopped-paying-complexity-tax-virtualization>.

⁴ See, e.g., <https://source.android.com/docs/automotive/virtualization>; https://source.android.com/docs/automotive/security/vehicle_system_isolation.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>network, including, for example, hypervisors (deployed in both QNX and Android-based systems) and/or operating system software modules (such as SELinux or equivalent mandatory access control software or process manager) that implement and enforce mandatory access control, packet filtering, and/or firewalls at the perimeter of a logical communication network and are operable to detect breaches.⁵</p> <p>Further, upon information and belief, the security measures employed by the '100 Accused Instrumentalities operating systems described above can determine whether a computational component affected by the instance of a breach of the security measure (i.e., upon detection of a malicious application attempting to violate a system security policy and/or gain access to forbidden resources and applications) can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure. For example, hypervisors enforce security policies between virtual machines and determine whether virtual machines affected by a breach can be isolated from other virtual machines. As another example, upon information and belief, process managers and mandatory access control software at the kernel level of the operating system detect attempts to perform disallowed actions, prevents disallowed actions at the kernel level, confines system services, controls access to application data and system logs, reduces the effects of malicious software,</p>

⁵ See, e.g., <https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/virt/virt.html>; <https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/network/network.html>; <https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/qhs/isolation.html>; <https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.hypervisor.safety.user/topic/qhs/isolation.html>; https://www.qnx.com/developers/docs/8.0/#com.qnx.doc.security.system/manual/security_features.html; <https://source.android.com/docs/core/virtualization/security>; https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.security.dev_guide/topic/manual/mac.html; https://www.qnx.com/developers/docs/8.0/#com.qnx.doc.security.system/manual/access_control.html; https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.adas.system_services/topic/sensor_security.html; <https://source.android.com/docs/security/features/selinux/concepts>; <https://emteria.com/blog/selinux-android>; https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.hypervisor.safety.user/topic/share_mem_config.html.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>1C</p> <p>(ii) determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and</p>	<p>and protects users from potential flaws in code on mobile devices.</p> <p>The network controller of the '100 Accused Instrumentalities determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.</p> <p>For example, upon information and belief, when a hypervisor, firewall, and/or mandatory access control software of the '100 Accused Instrumentalities detect a breach of a component within a logical perimeter network (e.g., unauthorized access to an operating system on a virtual machine or to an application within a sandbox), the software detecting the breach further determines whether the computational component affected by the breach can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure by selectively enforcing isolation actions via action of the firewall, process manager, mandatory access controller, or hypervisor.</p> <p><i>See also</i> Row 1B.</p>
<p>1D</p> <p>(iii) when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of;</p> <p>(a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure from the at least one on board computational component affected by the instance of a breach of the security measure;</p>	<p>When the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, the network controller of the '100 Accused Instrumentalities performs at least one of: (a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure from the computational component affected by the instance of a breach of a security measure and (b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure.</p> <p>For example, upon information and belief, the '100 Accused Instrumentalities use mandatory access control, sandboxing, and virtualization implemented by software executed by the</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>instance of a breach of a security measure and (b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,</p>	<p>network controller that can determine whether isolation of an affected component of a security breach is possible. This software can determine, for example, the processes, components, and surfaces affected by an attack, such as whether the attack is confined to a specific component (e.g., a sandbox or virtual machine), and determine the connections available between the affected component(s) and other components in the network that may be possible to isolate from the affected component.⁶ Upon information and belief, the '100 Accused Instrumentalities isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure, if it is determined that it is possible to do so,</p> <p><i>See also</i> Rows 1A-1C.</p>
<p>1E wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (4) activating a second security mechanism in response to the instance of a breach of a security measure.</p>	<p>In the network controller of the '100 Accused Instrumentalities, isolation of the computational component involves one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure.</p> <p>For example, upon information and belief, the '100 Accused Instrumentalities use mandatory access control, sandboxing, and virtualization implemented by software executed by the network controller to isolate components acting maliciously from one another and restrict communication to other on board components. This software is built into the '100 Accused</p>

⁶ See, e.g., https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.prog/topic/process_Procmgr_abilities.html; https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.security.dev_guide/topic/manual/sandboxing.html; https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.security.dev_guide/topic/manual/bestpractices.html;

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Infringing Activities
	and (4) activating a second security mechanism in response to the instance of a breach of a security measure.	Instrumentalities' operating systems and can, upon information and belief, deny connection or communication between components; halt the operation of an application at the kernel level of the operating system so that it cannot communicate with other applications; disable responses to broadcast pings; impose resource limits; set up network jails that isolate specific processes; activate additional security measures such as filesystem controls and memory managers; or otherwise isolate the affected component. ⁷
	Claim 2	<i>See also</i> Rows 1A-1D.
2	The vehicle of claim 1, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and/or network-accessible resource, wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAV 1, and/or WPAV2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle. Upon information	The '100 Accused Instrumentalities include the vehicle of claim 1, as described above. The '100 Accused Instrumentalities implement a network controller that detects and/or is notified of security breach instances that are one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and/or network-accessible resource, wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAV 1, and/or WPAV2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle. Upon information

⁷ See, e.g., https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.security.system/topic/manual/security_matrix.html; <https://source.android.com/docs/security/features/selinux/implementation>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>and a network probe, and wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAV 1, and/or WPAV2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate wireless signals from propagating outside the vehicle.</p>	<p>and belief, the network controllers in the '100 Accused Instrumentalities can detect many types of malicious attacks, such as malware, denial-of-service attacks, smurf attacks, buffer overflow, heap overflow, and the like.⁸ In response, the network controller may receive a warning signal from operating system software modules acting as a firewall, gateway, or impacted network node detecting activity inconsistent with a security measure, such as a violation of a security policy. On information and belief, the '100 Accused Instrumentalities implement security policies that include one or more of encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAV 1, and/or WPAV2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.</p> <p><i>See also</i> Claim 1, Rows 1B-1E.</p>
<p>Row</p>	<p>Claim 3</p>
<p>3</p> <p>The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational component, wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least</p>	<p>The '100 Accused Instrumentalities include the vehicle of claim 2, as described above.</p> <p>In the event of a breach, the computational component affected by the security breach instance can be an on board computational component, wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least</p>

⁸ See, e.g., https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.security.system/topic/manual/security_matrix.html; https://www.qnx.com/developers/docs/8.0/com.qnx.doc.security.system/topic/manual/security_matrix.html; <https://developer.android.com/privacy-and-security/risks/use-of-native-code>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Infringing Activities
	<p>expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.</p>	<p>one on board computational component are both within a perimeter network of the vehicle. Examples of components secured through this process include sensors used in the '100 Accused Instrumentalities' infotainment systems or elsewhere in the vehicle; critical safety systems and ECUs; non-critical devices such as radios; software applications in the infotainment system; processing modules in the infotainment system, a real-time operating system, or other vehicular system; or cellular upgrade module. Such components may be within the same perimeter network; for example, two software applications (one of which has been compromised by a breach of a security measure and one that has not) may be running on the same virtual machine within a particular perimeter network.</p> <p><i>See also</i> Claim 1, Rows 1B-1E.</p>
Row	Claim 7	
7	<p>The vehicle of claim 1, wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance are blocked in whole or part. For example, as described in Rows 1B-1E, in a scenario where at least one on board computational component in a vehicular wireless network has been affected and is in communication with another on board computational component that is not affected by the security breach instance, communications between the computational component affected by the security breach instance are, upon information and belief, blocked in whole or part.</p> <p><i>See also</i> Claim 1, Rows 1B-1E.</p>	<p>The '100 Accused Instrumentalities include the vehicle of claim 1, as described above.</p> <p>At least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance are blocked in whole or part. For example, as described in Rows 1B-1E, in a scenario where at least one on board computational component in a vehicular wireless network has been affected and is in communication with another on board computational component that is not affected by the security breach instance, communications between the computational component affected by the security breach instance are, upon information and belief, blocked in whole or part.</p> <p><i>See also</i> Claim 1, Rows 1B-1E.</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
security breach instance are blocked in whole or part.	
Claim 9	
<p>9A A method, comprising: in a vehicle comprising a plurality of on board computational components, a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components, and</p>	<p>The '100 Accused Instrumentalities perform the claimed method in vehicles that include a plurality of on board computational components and a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components.</p> <p>For example, the '100 Accused Instrumentalities have used several versions of the infotainment system software, including Sync 3, Sync 4, Sync 4A (the "Sync Systems"), and Ford Digital Experience ("FDE"). The Sync Systems are built on QNX platforms.⁹ FDE makes use of the Android Automotive Operating System ("AAOS").¹⁰ All of the '100 Accused Instrumentalities implement security mechanisms and logical perimeter networks around on board vehicle components through their in-vehicle software to enhance the safety and reliability of vehicles.</p> <p>For example, all '100 Accused Instrumentalities (Sync Systems and FDE) have a plurality of on board computational components, including (but not limited to) operating systems,</p>

⁹ See, e.g., <https://techcrunch.com/2014/12/11/ford-ditches-microsoft-for-qnx-in-latest-in-vehicle-tech-platform>; <https://www.forbes.com/sites/samabuelsamid/2019/10/30/new-ford-vehicles-to-get-sync-4-infotainment-and-ota-updates-from-2020/>.

¹⁰ See, e.g., <https://built-in.google/cars/>; <https://corporate.ford.com/articles/research-and-innovation/digital-experience>; <https://www.ford.com/technology/ford-digital-experience>; <https://www.ford.com/support/how-tos/ford-technology/ford-digital-experience/ford-digital-experience-profile-setup/>; <https://www.nickmayerfordeast.com/blogs/6941/the-new-android-powered-infotainment-system-in-the-2025-ford-explorer-in-cleveland-heights>; <https://www.youtube.com/watch?v=95w2mV4KJ9U>; <https://support.google.com/built-in/answer/9905854>; <https://support.google.com/assistant/answer/11091015>; <https://support.google.com/built-in/answer/13827211>; <https://support.google.com/My-Ad-Center-Help/answer/12155656>; <https://support.google.com/My-Ad-Center-Help/answer/12156161>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>electronic control units (“ECUs”), software domains, subsystems, and components.</p> <p>Upon information and belief, all ’100 Accused Instrumentalities (Sync Systems and FDE) include a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on-board computational components. This can be done in several ways. For example, upon information and belief, the Sync Systems and FDE each use various techniques for constructing logical communication networks that include on-board computational components and enforcing security measures at the perimeter networks to protect the integrity of the system. For example, upon information and belief, the ’100 Accused Instrumentalities including Sync Systems utilize firewalls, sandboxing and/or mandatory access control, and hypervisors to logically define perimeter networks around specific on-board computational components.¹¹ Security measures are implemented at these perimeter networks by, for example, defining security policies, which control what processes are allowed and where and which processes may connect with each other. The ’100 Accused Instrumentalities including FDE also use hypervisors, firewalls, sandboxing and/or mandatory access control to logically form perimeter networks around computational components and implement security policies at the perimeters.¹²</p>
9B a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance;	<p>The ’100 Accused Instrumentalities perform the claimed method using a microprocessor executable network controller that identifies a possible security breach instance. For example, upon information and belief, the ’100 Accused Instrumentalities include a microprocessor that runs software to enforce security policies for processes and communications at the interface of the perimeter network, including, for example, hypervisors (deployed in both QNX and Android-based systems) and/or operating system software modules (such as SELinux or</p>

¹¹ See, e.g., <https://www.iotevolutionworld.com/iot/articles/456299-blackberry-qnx-software-embedded-235-million-vehicles-worldwide.htm>; <https://seeingmachines.com/wp-content/uploads/2022/10/Hansen-Report-October-2018.pdf>; <https://www.es.bu.edu/~richwest/slides/CPS-IOTWeek-2022.pdf>; <https://www.redhat.com/en/blog/strategic-shift-how-ford-and-emirates-nbd-stopped-paying-complexity-tax-virtualization>.

¹² See, e.g., <https://source.android.com/docs/automotive/virtualization>; https://source.android.com/docs/automotive/security/vehicle_system_isolation.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>equivalent mandatory access control software or process managers) that implement and enforce mandatory access control, packet filtering, and/or firewalls at the perimeter of a logical communication network and identify possible security breach instances.</p> <p>Further, upon information and belief, the security measures employed by the '100 Accused Instrumentalities' operating systems described above identify attempts by malicious applications to violate system security policies and/or gain access to forbidden resources and applications, thereby identifying possible security breach instances affecting one or more computational components.</p>
<p>9C in response, the microprocessor executable network controller determining whether a computational component affected by the possible security breach instance can be isolated from at least one on board computational component not affected by or potentially affected by the possible security breach instance;</p>	<p>In response to identifying a possible security breach instance, the network controller of the '100 Accused Instrumentalities determines whether a computational component affected by the possible security breach instance can be isolated from at least one on board computational component not affected by or potentially affected by the possible security breach instance.</p> <p>For example, upon information and belief, when a hypervisor, firewall, and/or mandatory access control software of the '100 Accused Instrumentalities detects a possible security breach instance within a logical perimeter network (e.g., unauthorized access to an operating system on a virtual machine or to an application within a sandbox), the software detecting the possible security breach instance further determines whether the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance by selectively enforcing isolation actions via operation of the firewall, process manager, mandatory access controller, or hypervisor.</p> <p><i>See also</i> Row 9B.</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>9D when the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance, the microprocessor executable network controller at least one of (a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance from the computational component affected by the possible security breach instance and (b) isolating the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance,</p>	<p>When the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance, the network controller of the '100 Accused Instrumentalities performs at least one of: (a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance from the computational component affected by the possible security breach instance and (b) isolating the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance.</p> <p>For example, upon information and belief, the '100 Accused Instrumentalities use mandatory access control, sandboxing, and virtualization implemented by software executed by the network controller to effect isolation when it is determined that isolation of a component affected by a possible security breach instance is possible. This software determines, for example, the processes, components, and surfaces affected by an attack, such as whether the attack is confined to a specific component (e.g., a sandbox or virtual machine), and determines the connections available between the affected component(s) and other components in the network that may be isolated from the affected component.</p> <p>Upon information and belief, when it is determined that isolation is possible, the '100 Accused Instrumentalities isolate the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance.</p> <p><i>See also</i> Row 9A-9C.</p>
<p>9E wherein the isolation is one or more of:</p>	<p>In the '100 Accused Instrumentalities, the isolation is one or more of: (1) denying vehicular</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of wired equivalent privacy encryption, TKIP, EAP, LEAP, WPAv1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals from propagating outside the vehicle.</p>	<p>or denial of a computer network and/or network-accessible resource. Upon information and belief, the network controller receives warning signals associated with such security breach instances from one or more of a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and/or a network probe. For example, operating system software modules acting as firewalls, gateways, or process managers detect activity inconsistent with a security measure, such as a violation of a security policy, and provide corresponding warning signals to the network controller. Upon information and belief, the '100 Accused Instrumentalities implement first security mechanisms that include one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of wired equivalent privacy encryption, TKIP, EAP, LEAP, WPAv1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.</p> <p><i>See also</i> Claim 9, Rows 9B-9E.</p>
<p>Row</p>	
<p>11</p>	<p>The '100 Accused Instrumentalities perform the method of claim 10, as described above.</p>
<p>Claim 11</p>	

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>computational component affected by the security breach instance is an on board computational component, wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.</p>	<p>In the event of a breach, the computational component affected by the security breach instance can be an on board computational component, wherein the at least one on board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle. Examples of components secured through this process include sensors used in the '100 Accused Instrumentalities' infotainment systems or elsewhere in the vehicle; critical safety systems and electronic control units (ECUs); non-critical devices such as radios; software applications in the infotainment system; processing modules in the infotainment system, a real-time operating system, or other vehicular system; or cellular upgrade modules. Such components may be within the same perimeter network; for example, two software applications (one of which has been compromised by a breach of a security measure and one that has not) may be running on the same virtual machine within a particular perimeter network.</p> <p><i>See also</i> Claim 9, Rows 9B-9E.</p>
<p>Row</p> <p>15</p> <p>Claim 15</p> <p>The method of claim 9, wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security</p>	<p>The '100 Accused Instrumentalities perform the method of claim 9, as described above.</p> <p>At least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, where the communications do not normally pass through a gateway and/or firewall,</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the other on board computational component are, upon information and belief, blocked in whole or in part.</p>	<p>are redirected through and filtered by the gateway and/or firewall, and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part. For example, as described in Rows 9B–9E, in a scenario where at least one on board computational component in a vehicular wireless network has been affected by a security breach instance and is in communication with another on board computational component that is not affected by the security breach instance, communications between the computational component affected by the security breach instance and the other on board computational component are, upon information and belief, blocked in whole or in part.</p> <p><i>See also</i> Claim 9, Rows 9B-9E.</p>
Row	Claim 17
<p>17A In a vehicle comprising a plurality of on board computational components, a non-transient, tangible computer readable medium comprising a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components</p>	<p>The '100 Accused Instrumentalities include non-transitory, tangible computer-readable media in vehicles comprising a plurality of on board computational components and a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components.</p> <p>For example, the '100 Accused Instrumentalities have used several versions of the infotainment system software, including Sync 3, Sync 4, Sync 4A (the “Sync Systems”), and Ford Digital Experience (“FDE”). The Sync Systems are built on QNX platforms.¹³ FDE</p>

¹³ See, e.g., <https://techerunch.com/2014/12/11/ford-ditches-microsoft-for-qnx-in-latest-in-vehicle-tech-platform>; <https://www.forbes.com/sites/samabuelsamid/2019/10/30/new-ford-vehicles-to-get-sync-4-infotainment-and-ota-updates-from-2020/>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>makes use of the Android Automotive Operating System (“AAOS”).¹⁴ All of the ’100 Accused Instrumentalities implement security mechanisms and logical perimeter networks around on board vehicle components through their in-vehicle software to enhance the safety and reliability of vehicles.</p> <p>For example, all ’100 Accused Instrumentalities (Sync Systems and FDE) have a plurality of on board computational components, including (but not limited to) operating systems, electronic control units (“ECUs”), software domains, subsystems, and components.</p> <p>Upon information and belief, all ’100 Accused Instrumentalities (Sync Systems and FDE) include a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on-board computational components. This can be done in several ways. For example, upon information and belief, the Sync Systems and FDE each use various techniques for constructing logical communication networks that include on-board computational components and enforcing security measures at the perimeter networks to protect the integrity of the system. For example, upon information and belief, the ’100 Accused Instrumentalities including Sync Systems utilize firewalls, sandboxing and/or mandatory access control, and hypervisors to logically define perimeter networks around specific on-board computational components.¹⁵ Security measures are implemented at these</p>

¹⁴ See, e.g., <https://built-in.google/cars/>; <https://corporate.ford.com/articles/research-and-innovation/digital-experience/>; <https://www.ford.com/technology/ford-digital-experience/>; <https://www.ford.com/support/how-fos/ford-technology/ford-digital-experience/ford-digital-experience-profile-setup/>; <https://www.nickmayerfordeast.com/blogs/6941/the-new-android-powered-infotainment-system-in-the-2025-ford-explorer-in-cleveland-heights>; <https://www.youtube.com/watch?v=95w2mV4KJ9U>; <https://support.google.com/built-in/answer/9905854>; <https://support.google.com/assistant/answer/11091015>; <https://support.google.com/built-in/answer/13827211>; <https://support.google.com/My-Ad-Center-Help/answer/12155656>; <https://support.google.com/My-Ad-Center-Help/answer/9941814>; <https://support.google.com/My-Ad-Center-Help/answer/12156161>.

¹⁵ See, e.g., <https://www.iotevolutionworld.com/iot/articles/456299-blackberry-qnx-software-embedded-235-million-vehicles-worldwide.htm>; <https://seeingmachines.com/wp-content/uploads/2022/10/Hansen-Report-October-2018.pdf>; <https://www.cs.bu.edu/~richwest/slides/CPS-IOTWeek-2022.pdf>; <https://www.redhat.com/en/blog/strategic-shift-how-ford-and-emirates-ibd-stopped-paying-complexity-tax-virtualization>.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>perimeter networks by, for example, defining security policies, which control what processes are allowed and where and which processes may connect with each other. The '100 Accused Instrumentalities including FDE also use hypervisors, firewalls, sandboxing and/or mandatory access control to logically form perimeter networks around computational components and implement security policies at the perimeters.¹⁶</p>
17B	<p>The '100 Accused Instrumentalities include a microprocessor executable network controller on board a selected vehicle that, when executed. For example, upon information and belief, the '100 Accused Instrumentalities include a microprocessor that runs software to enforce security policies for processes and communications at the interface of the perimeter network, including, for example, hypervisors (deployed in both QNX and Android-based systems) and/or operating system software modules (such as SELinux or equivalent mandatory access control software or process manager) that implement and enforce mandatory access control, packet filtering, and/or firewalls at the perimeter of a logical communication network and are operable to detect breaches.¹⁷</p>

¹⁶ See, e.g., <https://source.android.com/docs/automotive/virtualization>;

https://source.android.com/docs/automotive/security/vehicle_system_isolation.

¹⁷ See, e.g., <https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/virt/virt.html>;

<https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/network/network.html>;

<https://www.qnx.com/developers/docs/7.0.0/index.html#com.qnx.doc.hypervisor.user/topic/qhs/isolation.html>;

<https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.hypervisor.safety.user/topic/qhs/isolation.html>;

https://www.qnx.com/developers/docs/8.0/#com.qnx.doc.security.system/topic/manual/security_features.html;

<https://source.android.com/docs/core/virtualization/security>;

https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.security.dev_guide/topic/manual/mac.html;

https://www.qnx.com/developers/docs/8.0/#com.qnx.doc.security.system/topic/manual/access_control.html;

https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.adas.system_services/topic/sensor_security.html;

<https://source.android.com/docs/security/features/selinux/concepts>; <https://emteria.com/blog/selinux-android>;

https://www.qnx.com/developers/docs/7.1/#com.qnx.doc.hypervisor.safety.user/topic/share_mem_config.html.

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>17C detects an instance of a breach of the security measure, determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and,</p>	<p>Further, upon information and belief, the security measures employed by the '100 Accused Instrumentalities operating systems described above can determine whether a computational component affected by the instance of a breach of the security measure (i.e., upon detection of a malicious application attempting to violate a system security policy and/or gain access to forbidden resources and applications) can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure. For example, hypervisors enforce security policies between virtual machines and determine whether virtual machines affected by a breach can be isolated from other virtual machines. As another example, upon information and belief, process managers and mandatory access control software at the kernel level of the operating system detect attempts to perform disallowed actions, prevents disallowed actions at the kernel level, confines system services, controls access to application data and system logs, reduces the effects of malicious software, and protects users from potential flaws in code on mobile devices.</p>
<p>17C detects an instance of a breach of the security measure, determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and,</p>	<p>The '100 Accused Instrumentalities include non-transitory, tangible computer-readable media storing instructions that, when executed by a microprocessor executable network controller on board a vehicle, detect an instance of a breach of a security measure. For example, upon information and belief, the '100 Accused Instrumentalities store instructions executable by a microprocessor to enforce security policies for processes and communications at the interface of the perimeter network, including, for example, hypervisors (deployed in both QNX and Android-based systems) and/or operating system software modules (such as SELinux or equivalent mandatory access control software or process managers) that implement and enforce mandatory access control, packet filtering, and/or firewalls at the perimeter of a logical communication network and detect breaches of security measures.</p> <p>Further, upon information and belief, the instructions stored on the computer-readable media cause the operating systems described above to detect attempts by malicious applications to violate system security policies and/or gain access to forbidden resources and applications, thereby detecting instances of breaches of security measures.</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>For example, upon information and belief, when a hypervisor, firewall, and/or mandatory access control software operating within a logical perimeter network of the '100 Accused Instrumentalities detects a breach affecting a computational component (e.g., unauthorized access to an operating system on a virtual machine or to an application within a sandbox), the executed instructions further cause the network controller to determine whether the computational component affected by the breach can be isolated from at least one on board computational component not affected by or potentially affected by the breach by selectively enforcing isolation determinations via operation of the firewall, process manager, mandatory access controller, or hypervisor.</p> <p><i>See also</i> Row 17B.</p>
<p>17D when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and at least one of isolates the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure from the computational component affected by the instance of a breach of the security measure isolates the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially</p>	<p>The '100 Accused Instrumentalities include non-transitory, tangible computer-readable media storing instructions that, when executed by a microprocessor executable network controller on board a vehicle, when the computational component affected by an instance of a breach of a security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, cause the network controller to perform at least one of: (a) isolating the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure from the computational component affected by the instance of a breach of the security measure and (b) isolating the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.</p> <p>For example, upon information and belief, the computer-readable media store instructions that, when executed, implement mandatory access control, sandboxing, and virtualization to effect isolation when it is determined that isolation of a computational component affected by a breach is possible. The executed instructions determine, for example, the processes, components, and surfaces affected by an attack, such as whether the attack is confined to a specific component (e.g., a sandbox or virtual machine), and determine the connections</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
<p>affected by the instance of a breach of the security measure,</p>	<p>available between the affected component(s) and other components in the network that may be isolated from the affected component.</p> <p>Upon information and belief, when it is determined that isolation is possible, execution of the instructions causes the '100 Accused Instrumentalities to isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.</p> <p><i>See also</i> Rows 17A–17C.</p>
<p>17E wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of the security measure, (2) directing communications to and from the computational component affected by the instance of a breach of the security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of the security measure, and (4) activating a second security mechanism in response to the instance of a breach of the security measure.</p>	<p>In the '100 Accused Instrumentalities, the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of the security measure, (2) directing communications to and from the computational component affected by the instance of a breach of the security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of the security measure, and (4) activating a second security mechanism in response to the instance of a breach of the security measure.</p> <p>For example, upon information and belief, the computer-readable media store instructions that, when executed, implement mandatory access control, sandboxing, and virtualization to isolate components acting maliciously from one another and restrict communication to other on board components. The executed instructions are built into the operating systems of the '100 Accused Instrumentalities and can, upon information and belief, deny connection or communication between components; halt the operation of an application at the kernel level of the operating system so that it cannot communicate with other applications; disable responses to broadcast pings; impose resource limits; set up network jails that isolate specific processes;</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>activate additional security measures such as filesystem controls and memory managers; or otherwise isolate the affected computational component.</p> <p><i>See also</i> Rows 17A–17D.</p>
Row	
18	<p>Claim 18</p> <p>The computer readable medium of claim 17, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, ARP spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource and wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11i, 802.11r, and/or 802.11s security, use of wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv1, and/or WPAv2 protocols,</p> <p>The '100 Accused Instrumentalities include the computer readable medium of claim 17, as described above.</p> <p>The computer-readable media of the '100 Accused Instrumentalities store instructions that, when executed by a microprocessor executable network controller on board a vehicle, detect and/or identify security breach instances that include one or more of: a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource. Upon information and belief, execution of the instructions causes the network controller to receive warning signals associated with such security breach instances from one or more of a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and/or a network probe. For example, operating system software modules executed pursuant to the stored instructions act as firewalls, gateways, or process managers that detect activity inconsistent with a security measure, such as a violation of a security policy, and generate corresponding warning signals to the network controller. Upon information and belief, the instructions stored on the computer-readable media implement first security mechanisms that include one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11i, 802.11r, and/or 802.11s security, use of wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv1, and/or WPAv2 protocols,</p>

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Infringing Activities
	addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.	end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle. <i>See also</i> Claim 17, Rows 17B-17E.
Row	Claim 19	
19	The computer readable medium of claim 18, wherein the computational component is affected by the security breach instance is an on board computational component, wherein the at least one on board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.	The '100 Accused Instrumentalities include the computer readable medium of claim 18, as described above. In the event of a breach, the computational component affected by the security breach instance can be an on board computational component, wherein the at least one on board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle. Examples of components secured through this process include sensors used in the '100 Accused Instrumentalities' infotainment systems or elsewhere in the vehicle; critical safety systems and electronic control units (ECUs); non-critical devices such as radios; software applications in the infotainment system; processing modules in the infotainment system, a real-time operating system, or other vehicular system; or cellular upgrade modules. Such components may be within the same perimeter network; for example, two software applications (one of which has been compromised by a breach of a security measure and one

**EXHIBIT J2 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Infringing Activities
	<p>that has not) may be running on the same virtual machine within a particular perimeter network.</p> <p><i>See also</i> Claim 17, Rows 17B-17E.</p>
Row	
23	<p>The '100 Accused Instrumentalities include the computer readable medium of claim 17, as described above.</p> <p>At least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, where the communications do not normally pass through a gateway and/or firewall, are redirected through and filtered by the gateway and/or firewall, and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part. For example, as described in Rows 17C-17E, in a scenario where at least one on board computational component in a vehicular wireless network has been affected by a security breach instance and is in communication with another on board computational component that is not affected by the security breach instance, communications between the computational component affected by the security breach instance and the other on board computational component are, upon information and belief, blocked in whole or in part.</p> <p><i>See also</i> Claim 17, Rows 17B-17E.</p>