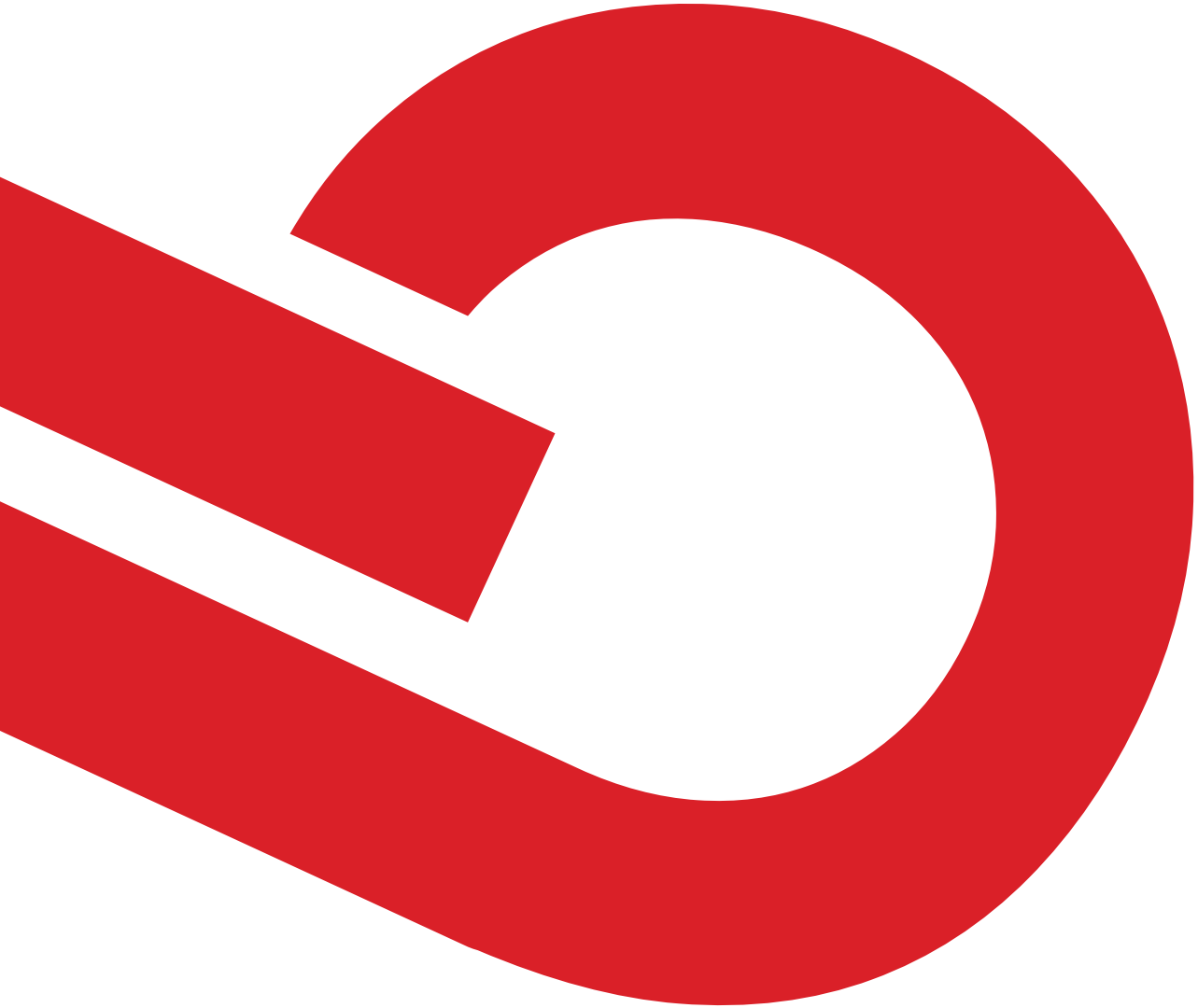


BUTZEL

TRUST. ALWAYS.

FALL 2021 REGULATORY AND COMPLIANCE UPDATE

GENIVI Fall Virtual All Member Meeting

Claudia Rast
rast@butzel.com
@RastLaw

Jennifer A. Dukarski, CIPP/US
dukarski@butzel.com
@JDukarski

BUTZEL
BUTZEL.COM

CYBERSECURITY UPDATE

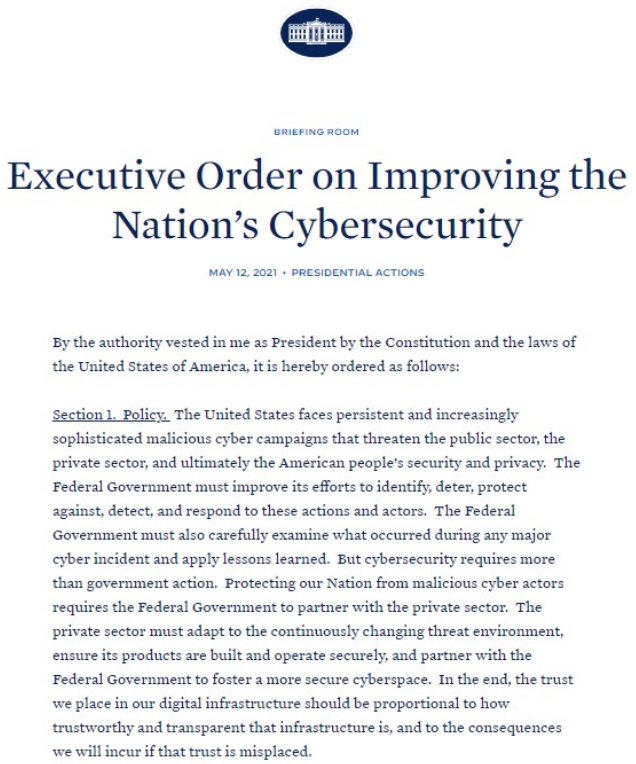
BUTZEL
BUTZEL.COM

What Is A “Critical Infrastructure?”

There are 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Transportation and Manufacturing are two of the critical infrastructure sectors with both asset and enterprise security being of critical importance.

Executive Order on Improving the Nation's Cybersecurity



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
- Improve Software Supply Chain Security
- Establish a Cybersecurity Safety Review Board
- Create a Standard Playbook for Responding to Cyber Incidents
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
- Improve Investigative and Remediation Capabilities

NIST / CISA – More Regulations to Come!

- Section 4 of the EO: “the Secretary of Homeland Security, in coordination with the Secretary of Commerce (through the Director of the National Institute of Standards and Technology) and other agencies, as appropriate, shall develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding o the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.”
- Preliminary cyber “performance goals” for control systems across critical infrastructure sectors are seen internally as a precursor to potential regulation of certain critical infrastructure operations.

Sanctions and Ransomware Payments

- ***September 21, 2021***: The US Department of the Treasury's Office of Foreign Asset Control (OFAC) issued an updated advisory related to the risks associated with ransomware payments
- "Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims."

Sanctions and Ransomware Payments

- For payments to entities or individuals on the Specially Designated Nationals and Blocked Persons List (the "SDN List") or to regional embargoes (Cuba, Crimea, Ukraine, Iran, North Korea or Syria) – you risk sanctions based on ***strict liability***
- Strict liability means any payment, ***even if you did not know!***
- OFAC encourages all victims to report ransomware attacks to CISA, the local FBI field office, the FBI Internet Crime Center or the local Secret Service office

NHTSA Cybersecurity Updates

- ***March 15, 2021***: Comments closed on the updated Cybersecurity Best Practices for the Safety of Modern Vehicles – an update from the 2016 first edition. 66 Comments were submitted.
- The update aligns and harmonizes with the UN Regulations on Cybersecurity and Software released in June 2020 and addresses:
  - Managing vehicle cyber risks
  - Securing vehicles by design to reduce risk in the supply chain
  - Detecting and responding to security issues throughout the fleet
  - Providing safe and secure software updates (OTA)
- The publication also identified 43 best practices and included 14 call-outs to ISO/SAE 21434

Considerations for Global Harmonization in Automotive Cybersecurity

- ***August 16, 2021***: China releases its first regulation on car privacy and data security (*Provisions on the Security Management for Automotive Data)* that included a broad scope of covered entities ranging from OEMs to online ride-hailing companies. Obligations appear to be based, in part, on the Fair Information Practice Principles (FIPPs)
- ***March 2021***: Meeting of the WP.29 World Forum for Harmonization of Vehicle Regulations under the UN Economic Commission for Europe (UNECE) which applies to 54 countries including Japan and South Korea (but not the US, Canada or China) proposal establishing a framework for software bill of materials

国家互联网信息办公室关于《汽车数据安全管理若干规定（征求意见稿）》公开征求意见的通知

2021-05-12 21:40 来源： 网信办网站 【字体：大 中 小】 打印

为加强个人信息和重要数据保护，规范汽车数据处理活动，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

1. 登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。

2. 通过电子邮件方式发送至：zqyj@cac.gov.cn。

3. 通过信函方式将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室，邮编100044，并在信封上注明“汽车数据安全管理若干规定征求意见”。

意见反馈截止时间为2021年6月11日。

附件：汽车数据安全管理若干规定（征求意见稿）

国家互联网信息办公室

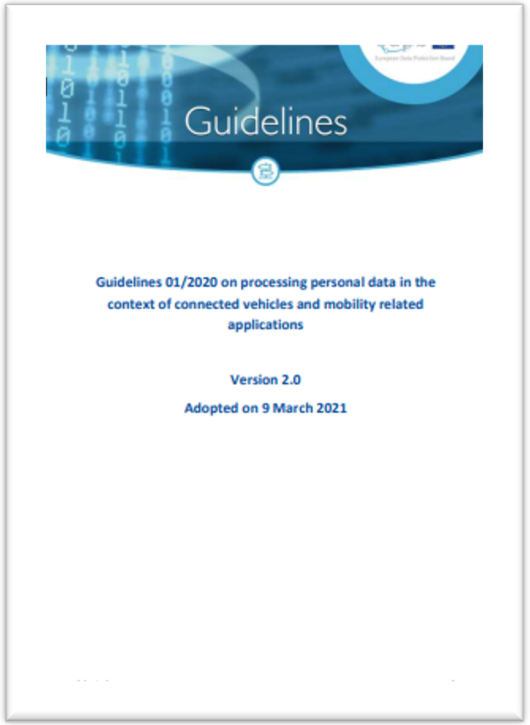
2021年5月12日

汽车数据安全管理若干规定

（征求意见稿）

第一条 为了加强个人信息和重要数据保护，规范汽车数据处理活动，维护国家安全和公共利益，根据《中华人民共和国网

EDPB Automotive Guidance



- ***March 9, 2021***: Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications are adopted
  - Encrypting communications with state-of-the-art algorithms
  - Encryption key management unique to each model
  - Regularly renew encryption keys
  - Authenticate data-receiving devices
  - Partitioning vital functions from those relying on telecommunications capacities (like infotainment systems)
  - Provide ability to operate vehicle in “downgraded mode” if attacked
  - Store a log history for a maximum of 6 months to allow for research on the origin of attacks

Pending Federal Cybersecurity Legislation

- S. 2407: Cyber Incident Notification Act
- S. 2201: Supply Chain Security Training Act
- S. 2439: Homeland Security Act Amendment - CISA Capabilities to Identify Threats to Industrial Control Systems
- HR. 4067: Communications Security Advisory Act
- HR 3138: State and Local Cybersecurity Improvement Act
- HR 1833: DHS Industrial Control Systems Capabilities Enhancement Act

And Perhaps Noteworthy: State Law Updates

- In 2021, 45 states and Puerto Rico considered more than 250 bills or resolutions that addressed cybersecurity.
- Hot topics in these bills include:
  - Requiring governmental units to implement training, draft formal policies, and plan for and test response to security incidents
  - Regulating within the insurance industry, including addressing cybersecurity coverage
  - Creating task forces
  - Creating incentives for cyber training and education

DATA PROTECTION / PRIVACY UPDATE

EDPB Redux: Auto Privacy Guidelines

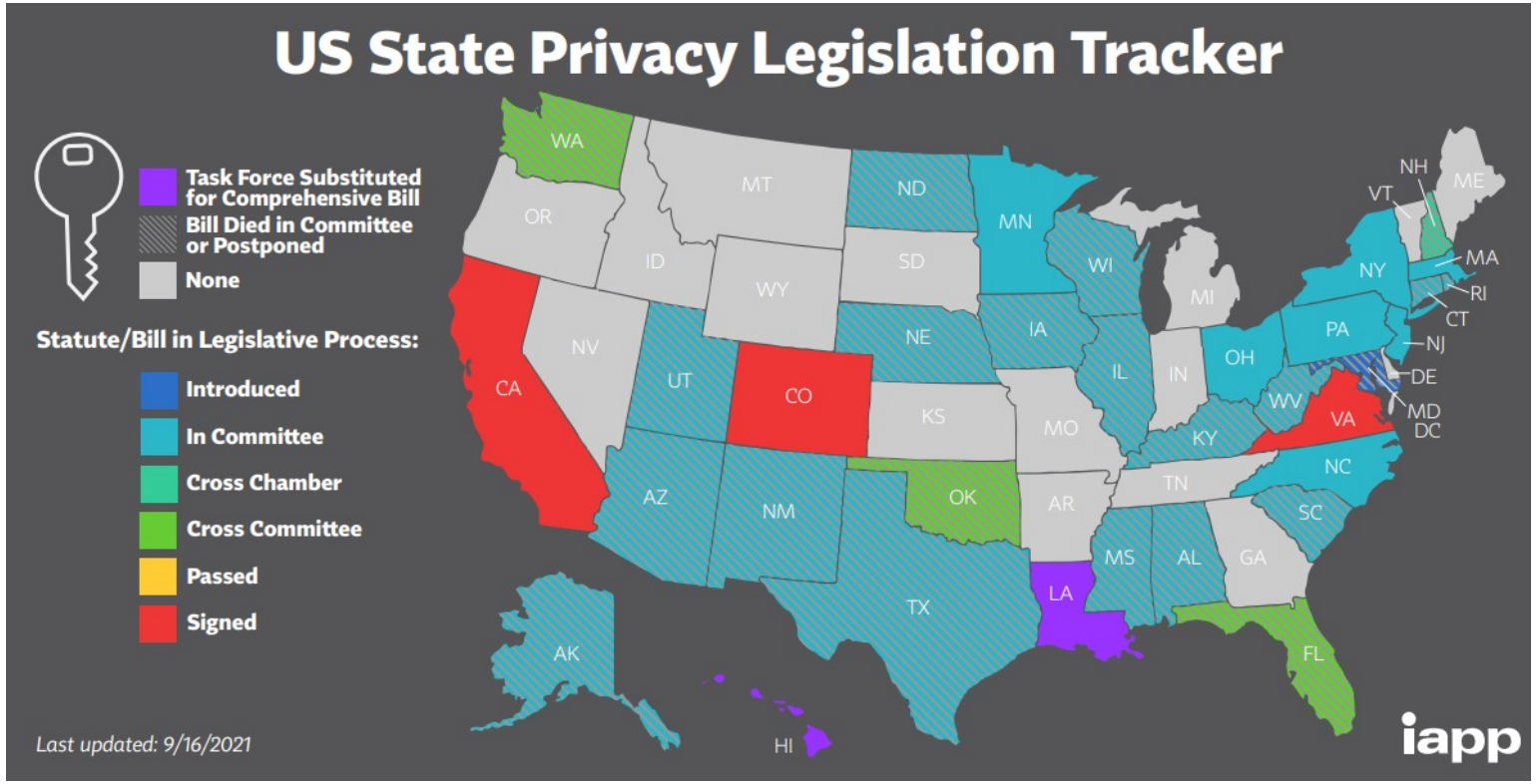
- Relevance and Data Minimization
- Data Protection by Design and Default
- Local Processing of Personal Data
- For Transmitted Data, Use Anonymization and Pseudonymization
- Perform a Data Protection Impact Assessment (DPIA)
- Inform Consumers of the Identity of the Data Controller, Purpose of Processing, Data Recipients, and Duration of Storage
- Implement a Profile Management System to Assure Rights of Data Subjects

Draft Federal Privacy Legislation

- Information Transparency and Personal Data Control Act
- Data Protection Act of 2021
- Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act)

Also Noteworthy: State Law Updates

- Enacted
  - California: CCPA / CPRA
  - Colorado
  - Virginia
  - Maine
  - Nevada
- Active Bills
  - Massachusetts
  - Minnesota
  - New York
  - North Carolina
  - Ohio
  - Pennsylvania



CASE LAW UPDATE

Exceeding Authorized Access to a Computer: *Van Buren v. United States*

- June 3, 2021 opinion of the Supreme Court
- The Computer Fraud and Abuse Act (CFAA), enacted in the 1980's, did not previously have its scope defined by the Supreme Court, specifically a provision prohibiting individuals from exceeding their "authorized access" to a computer
- In its decision, the court held that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him."

  Employee A has access to the company's HR database and uses that access to learn about co-worker salaries in order to negotiate for a raise.

  Employee B only has access to the company's intranet available to all employees but uses this access to "hack" into the HR database for a similar purpose.

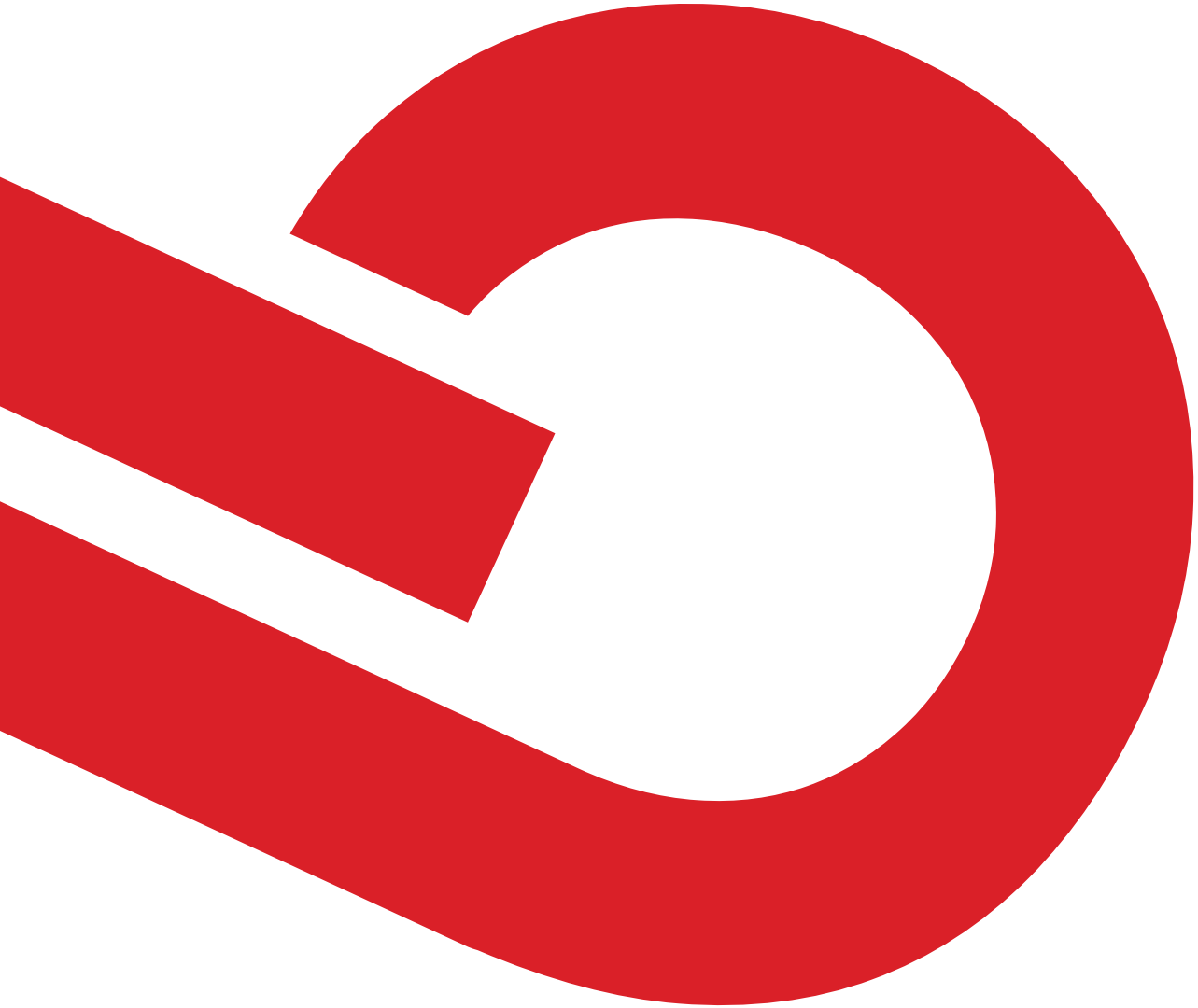
  Employee B has violated CFAA, but Employee A has not.

Privilege and Forensic Reports: *Guo Wengui v. Clark Hill, PLC*

- January 12, 2021 opinion of the DC District Court
- The court held that a forensic report created by forensic investigators and the associated materials were not protected by either the work-product or attorney-client privilege.
- Determining how a data breach occurs was held to be a necessary business function and couldn't be protected as a document prepared in anticipation of litigation.

Standing in Cybersecurity and Privacy Claims: *Flynn v. FCA*

- Pending before the 7th Circuit Court of Appeals
- Purchasers and lessees brought class action against vehicle manufacturer and component manufacturer, alleging that design flaws in vehicles' integrated phone, navigation, and entertainment control made vehicles vulnerable to hackers
- March 27, 2020: The Illinois district court dismissed for a lack of standing as the claims were too hypothetical
- October 27, 2020: Plaintiffs appealed to the Seventh Circuit where oral arguments were heard
- August 19, 2021: Supplemental authority memorandum filed with the court



BUTZEL

TRUST. ALWAYS.

Claudia Rast
rast@butzel.com
@RastLaw

Jennifer A. Dukarski, CIPP/US
dukarski@butzel.com
@JDukarski

BUTZEL.COM