RESEARCH BRIEF

Hacked Autonomous Vehicles: Who May Be Liable for Damages?

An Initial Investigation into How Civil Liability Systems Can Prepare

Autonomous vehicles (AVs) are intended to deliver a future of safer, easier transportation. Hackers, however, may interfere with that promise by attacking these heavy, fast, artificial intelligences on wheels and steering them toward mischief.

RAND researchers examined the liability implications should hackers gain access to AVs and sow mayhem. While the probability could be low, the stakes could be high, given that hacks on AVs could lead to deaths, property destruction, ransomware attacks, or theft of information.

The researchers found that existing civil liability law initially will likely be flexible enough to adapt to most legal claims arising from hacked AVs. Still, all parties involved in putting AVs on the roadways—manufacturers, owners, insurers, policymakers, and others—would be well advised to start thinking now about the risks, their liability implications, and both regulatory and statutory policy responses.

Adoption of the technology and its ability to pay social dividends depend not only on the actual risks but also on the *perception* of those risks and the legal structures that might compensate for them. Even if the risks are small, policymakers will need to anticipate and react to them to secure the potential benefits of AVs.

Key findings:

- Existing civil liability law is flexible enough to address most hacked autonomous vehicle (AV) claims.
- Makers of AVs and their component parts and software may face civil liability for criminal hacks on AVs.
- Product liability laws—along with warranty law and state and federal privacy laws—are the most relevant bodies of law.
- Manufacturers and operators should stay abreast of attacks on AVs and take precautions to avoid similar attacks and reduce liability exposure.
- Government agencies and infrastructure providers may also be found liable if their negligence creates an opportunity for a cyberattack.
- Some large-scale cyberattacks on AVs may not be insurable and could lead to uncompensated losses. Policymakers may wish to consider a government reinsurance backstop.

Envisioning an AV Future

AVs' promises—greater mobility for those who cannot drive, safer roadways, driving time dedicated to more-productive tasks—are spurring massive investment in the technology. Policymakers, in turn, are beginning to grapple with how to integrate AVs into society.

Along with such concerns as economic displacement of professional drivers, the specter of tens of thousands of cars running amok at the bidding of malicious hackers should give policymakers and AV advocates pause—even if its likelihood is small.

AVs are subject to multiple avenues of hacking attack. Software vulnerabilities, physical hacks via devices loaded with malicious code, and hacking of key hardware components all must be contemplated. These hacks can disable an AV, steer it toward destructive ends, and manipulate or steal user data, to name a few threats.

To assist policymakers in envisioning the civil legal implications of hacked AVs, RAND researchers investigated multiple plausible scenarios in which AVs could be hacked that resulted in some sort of loss that might be compensated through civil action.

Multiple Vulnerabilities

A number of scenarios that RAND researchers developed around hacked AVs helps illustrate the diversity of policy challenges facing the civil legal system, insurers, and others. These vignettes were generated by starting with real-world

hacking events or damages involving conventional vehicles and playing out scenarios to assist in liability analysis. They included

- a lone-wolf hacker accessing an AV's network to disable the car and demand ransom from the owner to restore its use
- a hacker taking control of a military officer's car parked on base and steering it to damage a military jet parked by a hangar
- hackers taking control of smart infrastructure that manages traffic lights and manipulating the signals to cause traffic accidents at intersections
- hackers planting malware in an AV owned by a car rental company that infects other corporate systems, resulting in the loss of customer credit card information, which is then used to make fraudulent transactions.

The civil liability of various parties was analyzed for these scenarios. That discussion identified the parties likely to be named as defendants in lawsuits arising from cyberattacks on AVs, focusing on

- AV manufacturers
- software manufacturers
- AV distributors
- AV owners and operators.

The Civil Law Backdrop

Because there are very few federal and state statutes on autonomous and connected vehicles, product liability laws—along with warranty law and state and federal privacy laws—are likely to be the most relevant bodies of law in suits arising from cyberattacks on AVs.

Negligence and strict liability are two legal theories that will play key roles in civil lawsuits arising from cyberattacks on AVs. Both of these theories involve balancing the foreseeability of specific cyberattacks and the costs associated with adopting alternative technologies that are less vulnerable to hacks.

Other areas of law that may shape liability in the context of hacked AVs include

- violation of consumer protection statutes
- misrepresentation, fraud, and fraudulent concealment
- warranty theories
- privacy laws.

Civil Legal Implications of Hacked AVs

The RAND researchers' application of the existing civil law framework to the scenarios they developed led them to multiple findings that will interest those shaping the future of AVs, including users, owners, manufacturers, insurers, and policymakers:

- AV manufacturers, manufacturers and designers of component parts and software, and distributors of AVs may face civil liability for the criminal hacks on AVs.
- Owners of AVs may also face liability for cyberattacks if, for example, they reject an important security update that allows a hacker to take control of the AV and cause damage.
- Existing civil liability law will likely be sufficiently flexible to adapt to hacked AV liability claims, at least for small- and medium-scale attacks.
- Because of the role of foreseeability in determinations of liability for the criminal acts of a third party (such as hacking), the issue of whether prior exploitation of a vulnerability was known will likely play a key role in liability determinations under existing civil liability law.
- In negligence and product liability cases, cost-benefit and foreseeability analysis will influence legal analysis of responsibility for damages from cyberattacks.
  - These cost-benefit analyses will require courts to become familiar with the technologies at issue.
  - Manufacturers of vehicles and component parts will need to stay abreast of attacks on AVs and take any necessary precautions to avoid similar attacks if they wish to avoid liability.
- Government agencies will be potential defendants in civil lawsuits that arise out of incidents involving unsafe infrastructure. Though there is considerable variation by state law, state and local governmental agencies will likely be protected by sovereign immunity as they adapt roadways to AVs. That immunity may not apply as they undertake ministerial tasks, such as road maintenance.
- After AVs and supporting infrastructure develop, government agencies will be more likely to be held civilly liable if their negligence provides the attacker an opportunity. Considerable state-by-state variation in sovereign immunity doctrine complicates the analysis.

Options for Policymakers

The finding that existing civil legal frameworks are likely to adapt to widespread introduction of AVs does not prevent policymakers from considering whether statutory approaches

that define roles and responsibilities would facilitate adoption of the technology.

Such a statutory framework might offer the benefit of clarifying duties but may be inflexible when compared with the common law system in the face of both hard-to-anticipate technological developments and novel fact patterns.

Similarly, it would be helpful to better understand and perhaps clarify insurance coverage for cyberattacks on AVs for both consumer and commercial policies so that consumers, automakers, and policymakers can better understand which parties will bear the costs of such attacks.

Policymakers may also want to carefully consider how the legal system might cope with a large-scale attack. Such an attack could lead to bankruptcies and uncompensated losses and could exceed the capacity of insurers and reinsurers to cover the risk. Similar concerns in the wake of the September 11, 2001, attacks led to the passage of the Terrorism Risk Insurance Act.

Will Consumers Care About Hacked AVs?

Unfortunately, consumers have grown accustomed to hacks that compromise their personal information. Cybersecurity breaches have not led to a strong consumer demand for increased cybersecurity. Thus far, consumers have shrugged, changed their passwords, and moved on. Hacked AVs, however, threaten a range of consequences that vastly exceed those of most consumer hacks in terms of potential for death and property destruction. This may lead to increased consumer incentives for cybersecurity of AVs.

RAND Ventures is a vehicle for investing in policy solutions. Philanthropic contributions support our ability to take the long view, tackle tough and often-controversial topics, and share our findings in innovative and compelling ways. RAND's research findings and recommendations are based on data and evidence, and therefore do not necessarily reflect the policy preferences or interests of its clients, donors, or supporters.

Funding for this venture was provided by gifts from RAND supporters and income from operations.

When Autonomous Vehicles Are Hacked, Who Is Liable?

Zev Winkelman, Maya Buenaventura, James M. Anderson, Nahom M. Beyene, Pavan Katkar, Gregory Cyril Baumann

This brief describes research conducted in the RAND Institute for Civil Justice and documented in *When Autonomous Vehicles Are Hacked, Who Is Liable?* by Zev Winkelman, Maya Buenaventura, James M. Anderson, Nahom M. Beyene, Pavan Katkar, and Gregory Cyril Baumann, RR-2654-RC, 2019 (available at www.rand.org/t/RR2654). To view this brief online, visit www.rand.org/t/RB10063. The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

www.rand.org

RB-10063-RC (2019)