AUTONOMOUS VEHICLES: A LEGAL VIEW

BRENT J. ARNOLD

April 29, 2021 ATC #*PrepareTogether*—Risks in Data: Cybersecurity and Threats

GOWLING WLG

AGENDA

Topic
Autonomous Vehicles and Cyber Risk
Who’s Liable When Something Goes Wrong?
Insuring Autonomous Transportation

AUTONOMOUS VEHICLES AND CYBER RISK

Examples

- May 2016 - Joshua Brown killed in a car crash while driving in a CAV;
- March 2018 - Wei Huang killed in a car crash while driving a CAV;
- March 2018 - Elaine Herzberg, a pedestrian, was struck and killed by an autonomous vehicle being tested by a rideshare service;
- March 2019 - Jeremy Banner was killed in a car crash involving a CAV inappropriately set on autopilot.
- April 2021 – Two persons killed in a Tesla in “full self-driving mode” with no-one in the driver’s seat

*Sources: https://gowlingwlg.com/en/insights-resources/articles/2020/cybersecurity-and-autonomous-vehicles/

AUTONOMOUS VEHICLES AND CYBER RISK

Types of Risk

- **Connectivity Risks**—Insecure network connections allow hackers access to CAV computers. Hardening these points is complicated because CAV software contains millions of lines of code, much of it based on legacy software and open source code. This makes vulnerabilities in CAV programs hard to find.
- **Automation Risks**—Vehicle sensors are possible attack vectors. Lidar sensor technology (used in most CAVs) is vulnerable to spoofing, and GPS can be jammed. Entire fleets of CAVs could be affected by malicious code embedded in mapping data or machine learning systems.

*Sources: https://gowlingwlg.com/en/insights-resources/articles/2020/cybersecurity-and-autonomous-vehicles/

WHO'S LIABLE WHEN SOMETHING GOES WRONG?

Basic theories of tort liability:

1. traditional negligence, under which the driver is liable for unreasonably failing to prevent a risk resulting in harm;
2. no-fault liability, under which accident victims are compensated by their own insurance and may not sue drivers unless their injuries reach a certain threshold,
3. strict liability, according to which vehicle operators are entirely responsible for abnormally dangerous or "ultrahazardous" operation of a vehicle.

*Sources: https://www.rand.org/pubs/research_reports/RR443-2.html

WHO'S LIABLE WHEN SOMETHING GOES WRONG?

European Union's Expert Group on Liability and New Technologies—Recommendations:

- **Strict liability** is an appropriate response to the risks posed by emerging digital technologies, if, for example, they are **operated in non-private environments and may typically cause significant harm**.
- **Strict liability** should lie with the **person who is in control of the risk connected** with the operation of emerging digital technologies and who benefits from their operation (**operator**)
- The **producer** should be strictly liable for defects in emerging digital technologies **even if said defects appear after the product was put into circulation**, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply.

*Sources: https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1

WHO'S LIABLE WHEN SOMETHING GOES WRONG?

European Union's Expert Group on Liability and New Technologies—Recommendations:

- **Operators** of emerging digital technologies should have to comply with an **adapted range of duties of care**, including with regard to (a) choosing the right system for the right task and skills; (b) monitoring the system; and (c) maintaining the system.
- **Producers**, whether or not they incidentally also act as operators…should have to: (a) **design, describe and market products** in a way effectively **enabling operators to comply** with the duties described above; and (b) **adequately monitor** the product after putting it into circulation
- Where the damage is of a kind that safety rules were meant to avoid, **failure to comply with such safety rules, *including rules on cybersecurity*, should lead to a reversal of the burden** of proving (a) causation, and/or (b) fault, and/or (c) the existence of a defect.

*Sources: https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1

INSURING AUTONOMOUS TRANSPORTATION

Insurance Bureau of Canada recommendations for insurers:

- Create policies that cover both driver- and automated technology-related negligence;
- Facilitate data-sharing between insurers, manufactures, and vehicle owners, to help determine the causes of a collision; and
- Update federal vehicle safety standards to incorporate new cybersecurity and technology standards.

*Sources: http://assets.ibc.ca/Documents/The-Future/Automated-Vehicle-Report.pdf

CONTACT

BRENT J. ARNOLD

Partner, Advocacy

Technology Sub-Group Leader (Com Lit)

T +1 416 347 2737
brent.arnold@gowlingwlg.com

Education

Osgoode Hall Law School (York University) J.D., 2005
Queens' University, M.A. 1999
York University, BA (Hons) (*summa cum laude*) 1994

Year of Call

Ontario Canada 2006

Brent J. Arnold is a partner practising in the Toronto office of Gowling WLG's Advocacy department, specializing in commercial litigation, data breach coaching and response, and data breach class action defence.

Brent is Vice Chair of the Steering Committee for the Cybersecurity and Data Privacy section of the U.S.-based Defence Research Institute (DRI), and sits on the executive of the Ontario Bar Association's Privacy and Access to Information Law Committee. He is corporate secretary for the Canadian chapter of the Internet Society, a global organization devoted to improving the affordability, accessibility, fairness and security of the internet.

Brent currently serves as a member of the court-appointed joint E-Hearings Task Force, whose mandate is to facilitate the modernization and re-opening of Ontario courts in the wake of the COVID-19 crisis.

GOWLING WLG

GOWLING WLG