1. My name is James Niles, I am the President, and Chief Innovation Officer of Orbit City Lab located in New York, NY USA. I would like to thank The House of Lords Science and Technology Committee for allowing me the opportunity to provide written evidence concerning autonomous vehicles. I would like to address questions 2, 3, and 13 with the following evidence.

2. It seems as if we all are “kids in a candy store” when it comes to the latest technology, and with autonomous vehicles, it is no different; we all want to peek inside the candy jar. For 99.9% of the public, the major benefits are safety improvement, road accident reductions, multi-tasking allowance, traffic lessening, or insurance reductions. Major concerns, which have been the focus of government agencies around the world, are vehicle safety issues, cyber security or data collection (privacy).

3. While safety, cyber, and privacy are important concerns, I want to talk about the proverbial elephant in the room that very few people are talking about but could potentially have a global impact if not addressed. This is the concern that autonomous vehicles could be used as a weapon (drone on wheels) which is very different from a cyber-attack. The House of Lords Science and Technology Select Committee needs to require that all autonomous vehicles have sensors installed inside the vehicle to perform a “sniff” test for hazardous/wmd material, and once detected, disable certain features of the autonomous vehicle.

4. It is not just I who believes that autonomous vehicles could be used a weapon, but perhaps more importantly several United States federal agencies and NATO believes it as well, yet no regulations have been implemented in any countries yet. An article that was published in 2014 makes reference to an internal Executive Analytic Report produced by the U.S Federal Bureau of Investigation that states the following on autonomous vehicles: “Autonomy will improve driving safety and make mobility more efficient, but will also open up greater possibilities for dual use applications and ways for a car to be more of a potential lethal weapon than it is today.”

5. Most recently, NATO’s deputy assistant secretary general for emerging security threats stated that “terrorist organizations are already working on creating their own autonomous vehicles to be used as a weapon”. Just how much effort do you think it would take for a group or individual to use an autonomous taxi as a weapon? Every major infrastructure around the world will now be less secured as the possibility of a bad actor using an autonomous vehicle as a weapon has increase dramatically.

6. For the most part, the concern that an autonomous vehicle could be used as a weapon has gone unnoticed by the public and probably by the majority of the government officials. In
2014 when the first article came out only a few other articles picked up and re-reported the finding. One article even argued against autonomous vehicles being used as a weapon because of the high price to acquire a vehicle and that would lead terrorist group/individuals to look for a cheaper approach. Given that on-demand autonomous taxi services will most likely be the introduction for the everyday consumer, this disproves the “too expensive” logic. Furthermore, having autonomous vehicles at airports, hotels, events, and roaming the streets increases the possibility that an attack could happen anywhere, all under the disguise of transporting a person from one location to another.

7. Aside from the safety, cyber, and privacy concerns mentioned previously, we need to look at mitigation for autonomous vehicles. The mitigation process aims to reduce the consequence of an incident by identifying best practices as well as codes or standards that make transportation infrastructure more resilient. Mitigation activities can include building to standards that enhance resilience, identifying risks, ensuring additional protection measures are applied to reduce vulnerabilities, and taking actions to reduce the consequence of incidents that may occur. Mitigation activities are arguably best applied in the planning stage instead of an afterthought or after an incident. Properly applied mitigation efforts can reduce the vulnerability to, or consequence of, an incident while making response and recovery efforts easier.

8. Keep in mind that just because you solve the cyber security concerns, does not mean that you have solved the issue of someone using an autonomous vehicle as a weapon. You could have the safest vehicle, the highest cyber security, and the tightest control of privacy data and still be wide open for bad actors to load the vehicle up with explosives, punch in coordinates, shut the door, and send the vehicle to its’ destination. All allowed as the current regulations have no requirement to prevent or mitigate the possibility of someone using the vehicle as a weapon.

9. Over the last couple of months, there have been numerous hearings from the intelligence communities worldwide; the major theme is not “if” something will happen but “when”. In today’s society, we need to be prepared, protect and mitigate risk against all possibilities regardless if it is from a single person or a group that may have intentions of causing harm or destruction. Country leaders from around the world look to each other for guidance on security and technology issues. Let us not make a bad decision that will have a rippling effect throughout the world.

10. Autonomous vehicles is a multi-billion dollar industry with numerous automotive and technology companies involved. Autonomous vehicles, parked in our garages, driveways, or as on-demand services such as autonomous taxis, create numerous possibilities, both good and bad. Automotive and technology companies would like to have fewer regulations and be able to freely develop and ask for exemption on regulations when it is in their best interest. However, security and protection should not be avoided or exempt just to allow faster to market so a few extra dollars can be made – the autonomous vehicle industry
should not be allowed to avoid regulations or achieve exemptions when it comes to security of the homeland.

11. In closing, if The House of Lords Science and Technology Committee do not require that autonomous vehicles have sensors to sniff out hazardous materials and then disable autonomous features once detected, you might as well start working on the speech that you will have to give to the world the day after an incident happens. Having to retrofit the vehicles after an incident, means an incident was successful. While a regulation will not eliminate all future terrorist attacks, there is no need to freely provide the opportunity to someone when in fact a reasonable mitigation solution is available.

12. The 9/11 Commission concluded that the greatest problem that lead to the attacks on 9/11 was “failure of imagination” on the government’s part. Let us fast forward our imagination down the road one, two or five years and think about how big of an impact that The House of Lords Science and Technology Committee decision to either implement or ignore a policy/regulation can have. Let’s not think back on today’s evidence and ask ourselves, “What-if....”.

*16 September 2016*