人类社会生产力的不断提高与工具的充分应用密不可分。从马车到蒸汽机，再到汽车都是对人类行动力的解放。正因为人类追求行动力解放的不懈努力，自动驾驶技术开始被广泛应用和开发。但随之而来的问题也是人们无法避免的，那就是数据安全和隐私安全，自动驾驶系统更像是一个人工智能，系统会收录司机的个人信息用以学习驾驶习惯，记录行程起点和终点，同时在驾驶的过程中会捕捉高分辨率的视频。试想一下，当自动驾驶技术被全面应用的时候，在每一秒都会有海量的数据产生。如何确保这些数据是安全的，以及基于用户隐私权的保护成为了必须面对的问题。本文将会从道德层面，法律层面，技术层面展开对自动驾驶隐私问题的探讨。并辅助以相关的例子证明我们的论点，描述如何做才是合理合法的数据利用，避免违法的数据披露和不当的数据使用。

关键词： 自动驾驶技术，人工智能，大数据，隐私保护，数据安全。

道德层面：

首先我希望从道德层面展开对这个问题的论述。

目前我们已知的自动驾驶技术，主要是收集司机的个人信息，例如姓名，性别，年龄，职业，家庭住址，公司地址，电话号码。其次会收集该司机所有的行程起点和终点，理由是为了合理的规划路线。为行驶过程中的周边环境进行录像，理由是通过学习周边环境来更好的训练自动驾驶模型。那么这个时候问题来了，司机是否知道自己的信息被收集了呢？被谁收集了？存储在哪？数据是否被滥用了？不幸的是，大部分用户对此一无所知。未知的数据收集和使用本身就是一个道德困境。自动驾驶系统每秒都会收集海量的信息，目的是通过数据的收集让系统变得更“聪明”，终极目的是为客户提供更好的服务。但是在收集的过程中，可能会无意的收集到用户的隐私信息，那数据的收集就应当被制止吗？明显不是，这种冲突的存在归根结底在于系统对于数据没有筛选收集的能力。

自动驾驶技术在道德层面的另一个困境就是，自动驾驶只会遵循自己学习到的规则去驾驶，举例来说，一个行人正在闯红灯穿过马路，如果是人为驾驶一定不会选择撞上去，可是AI的选择可能就是按交通规则驾驶。在自动驾驶发生车祸后，该由谁来负责？道德层面追求的普遍适应，往往希望得到最理想化的结果，看起来是行人的错误，但是道德上往往会倾向于弱者。换言之对于这样的问题，是道德无法解决的，因为道德无法将事故责任进行量化。

由于道德本身就是由人类所产生的，所以不管是数据的收集还是驾驶的规则学习，对于AI 来说都是一种没有任何倾向的行为。道德无法强加给AI的时候，责任的模糊化会让整个事件非常的复杂。在我看来，道德并不能作为界定对错的标准，因为道德本身不讲对错，只针对于特定的事情才会有对应的立场。比如数据的收集没有侵犯隐私，道德上认为AI是对的，一旦AI收集的数据牵涉到用户的敏感信息时，道德上就会对AI进行谴责。这其实是不公平的。再或者说，当行人闯红灯的时候，本身犯错的是行人，车辆撞上去发生的车祸，道德上就会谴责。当前有些自动驾驶公司为了避免这种情况选择让AI在这种情况下进行紧急刹车，或者是紧急避让。这可能让司机发生危险，道德还是会谴责这样的行为。道德是感性的，而AI是理性的，这本来就是两个互不兼容的事物。两者都无法强加给对方，但是两者其实都是为了一个目标所服务，所以寻求道德和AI的平衡成为了一个热门的话题。只有在兼顾道德的同时还能运作良好的AI才是人类所真正需要的技术。所谓的道德困境都是源自于技术的不足，法律的缺陷，当法律将对错量化，技术保障了基本道德不会崩坏，才是可以投入使用的成熟项目。这也是为什么后面会提到澳大利亚法律对于自动驾驶始终持一个谨慎态度的原因。

综上所述，自动驾驶技术的道德困境都来自一个问题，那就是自动驾驶技术无法从道德上将责任量化，道德更无法为该困境提供一个解决方案。这就是我下面要谈的，法律工具和技术工具。

法律层面：

依据上面提到的两个道德困境，我会从法律角度给出先行法律的解决方式，以及可能的解决方式。法律作为一种可以将对错量化的工具，一定是在确保公平，公正的前提下而实行的。这也是为什么道德层面解决不了的问题，往往可以从法律中找到答案的原因。

首先是第一个道德困境，自动驾驶需要收集海量的数据来训练AI，而不可避免会侵犯到用户的隐私。我从澳大利亚法律中对隐私原则的描述中找到了一些相关的条例。首先是澳大利亚要求APP实体必须以公开透明的方式管理个人信息。也就是说自动驾驶运营商在收集到用户的信息之后，所有数据的使用必须是公开透明的，这个条例很好的确保了即使客户的敏感数据被收集也不会出数据滥用的现象。同时辅助条例还提到，实体必须遵守澳大利亚隐私原则或者是此类守则的查询和投诉。也就是说客户可以对自己敏感数据滥用现象进行投诉，从而保护自己的数据安全。其次该法律条例中还提到，APP实体必须有明确的隐私政策，所有用户都有对其隐私政策了解的权力。这样在用户使用自动驾驶技术前，都可以阅读该公司声明会收集的信息以及未来数据的使用途径。在同意该公司的隐私政策之后才可以继续使用自动驾驶技术。最后法律条例还提到了对于敏感信息的处理，如果APP实体是一个组织的话，该实体不得收集个人信息，除非该信息对于该实体的一项或多项职能或活动是合理必要的。该条例明确说明了实体不得以除了训练AI之外的任何理由收集用户的敏感信息。这样就确保了用户的数据不至于被滥用或者是恶意的披露。

其次是第二个道德困境，也就是法律层面对于自动驾驶车祸的责任划分。目前南澳大利亚已经制定了允许无人驾驶车辆进行道路实验的法律。可以看到澳大利亚对于自动驾驶技术也是非常谨慎的，所有自动驾驶的汽车需要遵循实验指南在封闭路段进行测试，并且需要请求豁免法案，法律，或标准的初步指示，根据测试的结果反馈评估上路价值的可能性。对于评估合格的车辆，法律规定的第一个就是保险措施，使用无人驾驶的驾驶人需要对车，以及自身支付价值不菲的保险费用。与此同时对于车辆的豁免时间也有严格的限制。而且对于在豁免期间司机由于使用自动驾驶产生的任何事故，司机都要承担责任，处以罚款的判罚，情节严重的还会被起诉。鉴于当前的自动驾驶更多的是辅助驾驶，也就是说在事故发生前，司机是有能力手动制止事故的，所以司机也要承担法律责任。由此我们可以发现对于自动驾驶技术的普及，澳大利亚持保守态度，对于部分豁免的试验性质的自动驾驶技术，主要担负责任的还是车主。但是我相信随着自动驾驶技术的日益成熟，法律也会做出适应性的改变，当前的自动驾驶技术由于其不确定性而不被法律所承认和信任也是可以理解的。

下面我会就这两个问题在技术上展开我的探讨，主要目的是从技术层面上给出应对道德困境和法律限制的可能性，从而对自动驾驶技术的发展给出更多的可能性。

技术层面

自动驾驶技术当前的不成熟导致了其备受道德层面和法律层面的限制。我认为自动驾驶技术不成熟的主要有以下几点问题，首先是自动驾驶技术AI不够智能，主要还是以一个模式识别的方式去完成工作。第二是自动驾驶技术的传感器对数据的收集往往是无意义的，只要车主启动系统，就开始不停的收录数据，但其实往往收集到的都是无效数据，对于AI的训练和学习并没有关键性的作用。第三就是当前无人驾驶技术在驾驶过程中于其他汽车的交互，这种交互是不安全的。存在数据泄漏和被攻击的风险。下面我会就这三点分别给出一个例子并进行论证。

对于第一点，自动驾驶技术不够智能，我认为主要体现在三点，第一，自动驾驶技术只会机械化的学习规则，而不会随机应变。举例来说，自动驾驶收集到的天气预报数据显示今天会下雨，路上湿滑需要降速行驶。但是实际上今天并没有下雨，这时自动驾驶的慢速行驶就毫无意义。更加智能的AI应当是结合收集到的信息与当前传感器感知到的现实情况相结合，共同给出分析的结果。如果有所不同，一切应当是以显示传感器收集的实时数据为基准。这样也就能解决我们前面提到的有行人闯红灯的事情，当传感器传回的结果是有行人的时候，尽管当前是绿灯，也应当进行紧急刹车对行人进行避让。当这样的技术的实现成为可能的时候，自动驾驶技术的全面应用才有可能性。第二自动驾驶技术不懂得分辨数据是敏感数据还是可收集数据，前面提到自动驾驶技术的供应商是有自己的隐私政策的，那么依据于满足法律规定下的隐私政策同样应当被AI所学习。对于不该收集的数据要完全不收集，对于部分敏感信息，但是又需要学习的，可以将数据进行临时存储，在一定周期之后对数据进行完全删除操作。这样就避免出现侵犯用户隐私的现象。最后不够智能的体现就是，当前的自动驾驶都一套不成形的辅助驾驶规则，当自动驾驶完成普及，所有的车辆都是自动驾驶的时候，需要有一个能完全代替人去驾驶的AI存在。

对于第二点，传感器收集了大量的无效信息，浪费了大量的存储资源，以及很多无效学习消耗。我打个比方，我们今天学习了一个单词"苹果"，我们知道了这个单词的拼写方式和它的外观特征。那么之后每次遇到苹果我们都要重复一遍这个学习吗？答案很明显是否定的，只有当我们学习到苹果是红色的，有一天看到了黄色的苹果才需要进行二次学习。自动驾驶也是一样，以交通信号灯为例子，平时AI学到的只有红灯停，绿灯行，黄灯等一等，有一天信号灯停电了，但是AI认为这里有灯，这时候才需要AI的传感器全面开启，对没有信号灯的情况进行全面的学习，方便以后应对类似的情况。这样做的好处就是能够将大量的无效信息过滤掉，极大程度上节约了存储数据的空间以及无效学习的时间。更大的好处是一定程度上也减少了对一些无意识敏感信息的错误收集。

最后就是不同自动驾驶AI之间的交互，在自动驾驶汽车行驶的过程中，传感器会识别附近的车辆，并对对方的车辆进行数据收集和识别，举例来说，一条很狭窄的小路，只能同时通过两辆小型汽车或者是一个大型汽车，自动驾驶AI需要识别对面车辆是大型车辆还是小型车辆，从而做出继续驾驶或者是停车避让的判断，如果是救护车或者是正在出警的警车应当无条件避让的判断。在车辆交互的过程中，传感器不可避免地会收集到一些对方车辆的敏感信息。这很难说是好还是坏，举例来说，如果当前的AI识别出对方车辆是一个小型车，而我们当前驾驶的是大型车辆，对方应当避让，但是如果对方车上有孕妇马上要生产呢？从道德的角度上讲其实让对方先过去可能会拯救两条生命，但是从冰冷的AI判断上讲是不存在道德的。这样就又出现了一种难以调和的道德困境，无关于法律，但是却违背了道德的要求。另外一种情况就是在车辆交互的过程中，传感器可能会把对方驾驶员高清的照片进行拍摄传输，在澳大利亚的法律上来讲如果不对该照片进行恶意的披露，本身传感器的拍摄是不违法的，但是如果收集到的信息被恶意利用了呢？这样的敏感信息的披露将会变得不可控。从技术层面上来说，这时候自动驾驶公司往往会选择使用假设验证的方法去处理。所谓假设验证就是对当前的情况进行一个假设，称为H0，在当前情景下我们的假设是传感器对收集到的敏感信息不会出现泄漏，滥用的情况。之后公司需要从大量的数据中应用统计学的方法去采样。一般情况下我们认为小概率事件就等于不会发生，但是如果在采样检测的过程中出现了信息滥用或信息泄漏，则认为传感器拍摄到的敏感信息会被泄漏或者是滥用。

综上所述，无论是道德困境还是法律要求，技术本身都可以最大程度的解决这些问题，但是会有优先处理，即技术倾向于优先解决法律要求，因为这涉及到后续是否可以使用自动驾驶技术。在道德层面上，需求往往难以判断。比如早上上班堵车的时候，我们有时会选择礼貌地让一些车通过。对方也会招手表示感谢。这种习惯习惯通常不被 AI 理解。 AI的处理逻辑单一，只会按照指令完成行为，会无视人与人之间的道德规则。因此，只有当技术变得足够智能，从目前的伪人工智能到真正的人工智能，也就是当人工智能能够像人类一样拥有情感和思维能力时，这些道德问题才能得到解决。

最后，我认为自动驾驶技术的应用是必然的，这是一把双刃剑，技术的空前发展必然会带来争议和矛盾。在第二次工业革命之后，汽车的广泛普及也带来了很多道德和法律层面的争议，随着汽车的稳定性，安全性全面提升，道德上慢慢会形成适应的新的道德准则，而法律更是会因势利导构建起一套完善的法律条例去保护人类的权益。在我们面对第三次工业革命时，也就是现在的信息革命。主要特征就是数据的爆炸性的增长，让各个领域充满了未知的可能。在我看来自动驾驶技术就是信息革命的典型体现，不仅仅是技术层面的提升，更多的是展现了人类对于美好未来的不断探索和努力。但我们也要保持警惕，越来越多的数据问题让现代人成为了‘裸体’，在大数据面前，一个人的喜怒哀乐，关系网络都一览无余。保护数据的安全，保护人的隐私始终是任何技术都要尊重的基本权益，因为任何技术或道德，或法律，最终服务的对象都是人。