The Critical Legal Contention under the Challenge of Information Age and the Predominant Social Interests Concern for Developing Intelligent Vehicle Telematics in the United States

Fa-Chang Cheng
National Kaohsiung First University of Science and Technology/Graduate Institute of Science and Technology Law, Kaohsiung City, Taiwan
Email: fachang1@hotmail.com

Wen-Hsing Lai*
National Kaohsiung First University of Science and Technology/Dept. of Computer and Communication Engineering, Kaohsiung City, Taiwan
Email: lwh@nkfust.edu.tw

***Abstract*—Intelligent Vehicle Telematics has been a promising industry in the world. This new development of telecommunication technology has emerged with some legal concerns, especially in the liability for failure of safety devises and the protection of information privacy within Intelligent Vehicle Telematics. The purpose of this article is to gain experiences from the discussion for these concerns in academic papers and related cases within the United States, in order to depict the possible solution for safety related legal concerns and the protection of information privacy which is based upon not only the concern of information age but also the concern of national security with regard to developing Intelligent Vehicle Telematics. The purpose of this article is intended to offer some valuable reference to other countries which are also involving in the development of intelligent Vehicle Telematics.**

***Index Terms*—Intelligent Vehicle Telematics, product liability, strict liability, information privacy**

I. Introduction

The Intelligent Vehicle Telematics is highly valued by the government in the world as having a lot of beneficial potential to the transportation infrastructure in such sovereignty. The features of safety design are critical to the Intelligent Vehicle Telematics and have some significant meaning to the legal infrastructure. Those safety devises may increase the safety of transportation which benefits to the society as a whole. Conversely; the failure of such safety devises may cause a lot of trouble. Therefore, the liability for system provider and devise manufacture (distributor) is one significant safety legal issue with regard to Intelligent Vehicle Telematics. Apart from the safety related legal concerns, the protection of privacy in the operation of Intelligent Vehicle Telematics is also another critical legal issue for Intelligent Vehicle Telematics. The intention of this article is to introduce the concept of information privacy in the United States and bring up the suggestion of how to comprise the conflictions between protecting information privacy and other legal interests. Since this paper is mainly talking about the concerns from the prospective of the United States because due to the United states advancing in Intelligent Vehicle Telematics research field, except the general technology description of Intelligent Vehicle Telematics, including the safety features, in the beginning, this article will center the discussion on these concerns to academic papers and related cases within the United States, in order to depict the possible solution for safety related legal concerns and the protecting privacy concerns with regard to developing Intelligent Vehicle Telematics to other following countries.

II. The Technology of Intelligent Vehicle Telematics and its Safety Features

Vehicle Telematics is the integrated use of telecommunications and informatics within road vehicles. The objectives of Intelligent Vehicle Telematics are to improve safety, reduce traffic congestion, fuel consumption and carbon dioxide emissions, and increase comfort and convenience or even entertainment, and the future trends focus on making automobiles greener, smarter, and merging transportation and information

Manuscript received September 20, 2012; revised September 20, 2012; accepted September 20, 2012.
* Corresponding author

doi:10.4304/jcp.8.6.1552-1559

networks [1]. Most vehicle telematics projects were developed isolate. However, in some regions, like European Commission, have decided to act forwards harmonizing the deployment and use of ITS in road transport across Europe by means of the ITS Action Plan and the European ITS Directive [2].

Wireless communications and networking is a core enabling technology for ITSs (intelligent transport systems). A vehicle may communicate with other vehicles (vehicle-to-vehicle, V2V) or the infrastructure (vehicle-to-infrastructure, V2I) by using Dedicated Short Range Communication (DSRC), cellular communication, satellite communication, WiFi, Bluetooth or RFID. Among them, DSRC is short to medium range wireless communication promoted by US Department of Transport and specifically designed for vehicle use. US Federal Communications Commission (FCC) has allocated 75MHz in the 5.9GHz band for DSRC. Longer range communications can be accomplished by GSM, 3G, or WiMAX. It is noted that to prevent accidents, very low latency and short response times are needed for vehicle-to-vehicle communications [3]. IEEE 802.11p, which is the groundwork for DSRC, is an IEEE standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 to support ITS. That is, it is specially designed for data exchange among moving vehicles and road infrastructure.

Generally speaking, in vehicle transportation, safety normally gets top priority, though entertainment and convenience have rapidly caught up to safety as the impetus for new in-car electronics development [4]. Examples of many applications of vehicle safety systems are: Cooperative forward collision warning, Emergency braking notification, Lane or road departure warning, Pre-crash sensing, Curve speed warning, Right turn assistance, Give way junction assistance, Traffic signal violation warning, Intersection collision warning, Road / rail collision warning, Road condition warning, Approaching emergency vehicle warning, Emergency vehicle signal pre-emption, Road works warning, and Motorway merge assistance [5].

The above safety related application systems or functions of intelligent vehicle system generally focuse on assisting drivers and preventing driver errors while full autonomous, unmanned vehicles are still remained as a research topic. However, these systems which designed to improve safety may, instead, compete for driver attention and provide confusing message [6]. That causes the telematics use becoming a contributing factor for crashes, mostly due to multitasking, distraction and longer duration usage time than conventional in-vehicle tasks [7]. Besides, more and more car innovations are from computer systems and software, and such complexity brings with it reliability concerns [8]. Ivan Berger [9] questioned three growing challenge for carmakers. First, the more complex a car electronic system, the more failure points it offers. Second, the growing reliance on software raises more risk of fail. Third, the hardware environment becomes more demanding because of heat and electromagnetic interference (EMI).

Some methods have been proposed to solve the safety concerns. For example, a workload manager is set to help determine if a driver is overloaded or distracted [7], and a structured procedural safety assessment of intervening systems is proposed [10]. Nevertheless, unless we can totally understand the driving behavior [11] - [13], including driver intentions, how people make decisions, and how people interact with vehicle, and model the behavior, there are still risks.

In addition, there is privacy concern to aware. Knowing the accurate position and status of vehicles is the first thing to do to make the transport intelligent. Global Positioning System (GPS) is a convenient way to calculate the information. However, the accuracy of standard GPS, which is generally 5 to 10 meters, is not always enough, and the accuracy and reliability of GPS are degraded in urban environments due to satellite visibility and multipath effects. Other technologies like Triangulation Method using mobile phones or inertial navigation by the sensors via dead reckoning could be integrated to improve the accuracy. Video cameras can also be fused [14] to help measure traffic flow or the distance between lane lines. The computer vision technology can not only be used to look out of the vehicle to detect and track roads, but simultaneously look inside the vehicle to monitor the attentiveness or intentions of the driver [15]. Besides camera, multiple Sensors including radar and lidar can be used to help detect various statistic or moving on-road obstacles [16]. Using standard statistics of telecom switches without extra effort in telecom network is also used to compute the speeds of vehicles [17]. By using the above techniques, accurate position or status information is obtained and then, these information is generally shared with other vehicles and infrastructure by communication. If privacy filtering is not applied, serious privacy risk happens. Some applications like Pay-As-You-Drive Insurance model [18] have noticed it. The system performs the premium calculations locally in the vehicle, and send only aggregated data to the insurance company without leaking location information.

Another trend to aware is that cloud computing is expected to play a pivotal role in future automotive telematics services. It particularly makes the security and privacy in clouds an important issue in ITS.

III. THE LIABILITY OF SYSTEM PROVIDER AND DEVISE MANUFACTURE (DISTRIBUTOR) FOR SAFETY LEGAL CONCERNS

The safety concern for the Intelligent Vehicle Telematics is by far the most concerned topic both from the technical and the legal perspective. Discussing from the legal perspective for safety concern to Intelligent Vehicle Telematics, at first sight, there could be three potential possible kinds of liability, negligence, warranty in contract or strict liability, for the system provider and four potential possible kinds of liability for devise manufacture (distributor) with regard to the safety legal

concerns, adding product liability to the three just mentioned before. The difference between the system provider and the devise manufacture (distributor) for potential liability to the safety legal concerns the product liability because the product liability is only eligible for the harm done by the tangible product, but not the services. For the purpose of elucidating the discussion here, briefly introducing the concepts of negligence, warranty, strict liability and product liability is necessary. And the assertion of this article will insist that strict liability theory is most appropriate to those situations based on the understanding and characteristics of those legal infrastructures since there is no real case handed down related to the safety legal concerns for Intelligent Vehicle Telematics in the United States judicial system. Regarding this section here, the discussion will be divided into three parts discussion: the first part of theories among negligence, warranty, product liability and strict liability; the second part of comparing among negligence, warranty, product liability and strict liability for the culpability; and the third part of the reason to choose strict liability for the system provider and devise manufacture (distributor) as the liability solution for the related safety legal concerns to Intelligent Vehicle Telematics.

A. The Theories among Negligence, Warranty, Product Liability and Strict Liability

The first safety liability theory for system provider and devise manufacture (distributor) to Intelligent Vehicle Telematics is negligence. Generally speaking, the theory of negligence is really based upon the idea of fault. To indicate a defendant is negligent means that the defendant in the case violates the duty of care imputed by the society. And, except for some specific circumstances, the standard of care is either based upon the reasonable person [19] or professional reaction [20] under the ordinary cases. Another specific feature for the theory of negligence is the requirement for proximate cause of which the legal meaning is to define the amount of damages. The cause in fact between the wrongdoer and the consequences invoked by such wrongdoer is required in every tortious cause of action, the proximate cause is not a prerequisite for the cause of action in torts, for example the intentional torts or product liability etc. and the proximate cause is really a means to the policy concern's ends [21]. So, in order to substantiate in a negligence case, there are four elements need to be proved: duty of care, breach duty of care, causation (including the cause in fact and proximate cause) and damages.

The second possible legal theory of the liability for system provider and devise manufacture (distributor) related to the safety devise for Intelligent Vehicle Telematics is warranty. Warranty cause of action is really something between the contract theory and the torts theory. Two kinds of warrant theory fall under this category; one is called the express warrant, the other is named the implied warranty. In the express warranty, it could be the contract liability which needs to prove the contract privity between the parties involved in the warranty dispute. The express warrant could also be the torts liability which needs to prove the reliance of the injured party, even though there is no requirement for proving the privity between the parties [22]. And the adoption of implied warrant theory is, to some extent, depending on the willingness of the court and mostly used in the dispute of fitness of the object to its common application [23].

The third possible legal theory to the mentioned liability is strict liability. In the strict liability theory, there is no need to prove the defendant's fault, the contract privity, the reliance of the injured or even pending on the court's interference. To prove some basic facts and establish that these facts results in the consequences is the only requirement to assert the strict liability. Traditionally, two types of strict liability are accepted in cases: the wild or vicious animal strict liability and the extremely dangerous activity strict liability. However, even under this stringent liability, some exceptions exist to the general rule, like the comparative negligence of plaintiff [24] or the Act of God [25].

The last possible legal theory of the liability mentioned in this paragraph for system provider and devise manufacture (distributor) related to the safety devise for Intelligent Vehicle Telematics is product liability. The main purpose of product liability is to protect the user or consumer from injured by the product threw in the stream of commerce. Theoretically, this legal theory contains three different types of product liability claims: manufacturing defect, design defect and lack of warning [26]. Several possible legal interpretations can delineate the meaning of product liability. To make the statement more clear, under the title of product liability, a product liability case can really be a negligence case [27], a warrant case [28] or a strict liability case [29]. When a product liability case is based upon the strict liability theory, the distributor or the manufacture for the product would easily be involved in such case. The provision in the Restatement (Second) of Torts embodies the strict liability approach. According to Restatement (Second) of Torts § 402A which is accepted by some of the states in the United States, one who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, even the seller has exercised all possible care in the preparation and sale of his product or the user (or consumer) has not brought the product from or entered into any contractual relation with the seller. Even the Restatement (Second) and following courts take the position that both the manufacture and the distributor shall bear the strict liability [30], there are still some jurisdictions which partially follow the Restatement (Second) would like to prove the breach of duty to the manufacture which is based upon design defect and lack of warning claims in a product liability litigation [31]. And just similar to the strict liability, there are also a couple possible defenses, comparative negligence of plaintiff [32] and statutory immunity (preemption) [33] or

unforeseeable misuse of the product [34], could be used as the defense against the product liability. To sum up the description regarding the product liability, the product liability is the liability to harm caused by the product which liability can present either one of the three possible choices: negligence, breach of warranty or strict liability.

B. The Comparison among Negligence, Warranty, Product Liability and Strict Liability for the Culpability of Wrongdoer

From the explanation in this previous paragraph, the conclusion for comparing different legal theories for the safety related legal dispute can be summarized as the following. First of all, the negligence cause of action is the most difficult liability to prove because, unlike warranty or strict liability, the duty of care needs to be substantiated. And the strict liability might be the easist legal theory to satisfy in the burden of providing evidence. As to the warranty cause of action, the liability would either rely on the contract privity or reliance in express warranty or count on the court intervention in implied contract. To estimate the strength of liability or culpability, the warranty cause of action seems to stand in between of the negligence and the strict liability. The last possible liability mentioned in this article-product liability, is really a mixture type of theory of liability among the negligence liability, warranty liability and the strict liability. Observing the history of the policy attitude toward the product liability, the substance to contend product liability is really swinging between the negligence and the strict liability and some commentator believes the current court attitude in applying the product liability is more lenient toward the manufacture [35].

C. The Reason for Choosing Strict Liability for the System Provider and Devise Manufacture (Distributor) as the Liability Solution for the Related Safety Legal Concerns to Intelligent Vehicle Telematics

This article would like to indicate that those safety devises to Intelligent Vehicle Telematics are presenting really high social responsible concerns. Therefore, the primary policy thinking should be that the manufacture of these safety devise to Intelligent Vehicle Telematics is going to hold the highest legal responsibility under the current legal theory to the injured person or property based upon the strict product liability. And the system provider for the operation of these safety devises to Intelligent Vehicle Telematics is the same important as the manufacture. If anything goes wrong with the system, it could cause a catastrophe to the transportation. Therefore, the system provider for the operation of these safety devises to Intelligent Vehicle Telematics should also take the strict liability. The liability for both the manufacture and the system provider here is nothing like the liability to the cell phone manufacture or the communication services provider for the user talking over the cell phone while he or she was driving because the cell phone is not designed to the protection of transportation safety and the user who initiates communication and cause the distraction which results in the traffic incident should be responsible for his or her behavior [36]. As to the distributor between the manufacture and the user or consumer, because the distributor doesn't directly contribute to the safety legal issue regarding the safety devises within Intelligent Vehicle Telematics, it is suggested the distributor doesn't need to be strictly liable to the injury based upon product liability by the failure of these safety devises. The current situation as to different options for liability to the distributor should remain the same for further consideration through the case decision in the future.

IV. THE PROTECTION OF INFORMATION PRIVACY IN INTELLIGENT VEHICLE TELEMATICS

As mentioned in the beginning of this article, in applying Intelligent Vehicle Telematics to the real world, often times, it will acquire, collect or use personal information in the process of operating these devises or systems. This could arouse a lot of concerns to the legal issue of information of privacy. In this section, it intends to introduce the idea of information privacy in the United States, the protection of this legal interest in the United States. Not only will several inclined tendencies to the protection based on the concern of information age be indicated here but also is the suggested hierarchy of methods to build up such protection in the legal arena for Intelligent Vehicle Telematic going to be discussed. One additional future possible concern to the protection of critical infrastructure based upon the reason of national security will also be briefly discussed for the purpose of this article. The purpose of all these discussions is to make projection of what would have happened if the issue of information privacy emerged once the industry of intelligent vehicle telematics becomes mature.

A. The Concept of Information Privacy and the Protection in the United States

The protection of "privacy" is not articulated in the Constitution in the United States, instead it is interpreted by the Supreme Court to say "The forgoing cases suggest that special guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy." in order to "create" the protection of privacy [37]. Through the years, the Supreme Court has recognized several kinds of privacy as the fundamental human rights [38], for example the right to marriage, breeding the child etc., but not the information privacy. The significant legal meaning of information privacy as a non-fundamental human rights on the Constitutional level is that the right of privacy will probably be restricted when it directly conflicts with the protection of other fundamental human rights or important social rights, for example the freedom of speech [39]. And it is fairly to say, other than conflicting with the protection of other fundamental human rights or important social rights, the protection of information privacy is really the balance of interests between the protection of privacy and other affected legal interests, except it wouldn't affect any legal interests, for example, to the protection against unauthorized invasion of

information privacy. From the experience of the United States in protection of information privacy, there are three auspicious preventive and one remedial trends worth to draw attention. The first preventive trend is to use informed consent mechanism for reducing or eradicating the controversy of reasonable expectation of privacy. The second preventive trend is to emphasize the importance of technology prevention of information privacy infringement. And the last one preventive trend is to enhance the liability of data collector for notification of the security breach to the information provider in case of some special kind of personal information been unauthorized disclosed by the third party. As to the remedial trend related to the protection of information privacy for intelligent vehicle telematics, the focus will be the secondary liability to the internet service provider. Especially a secondary liability case of internet service provider about trademark infringement in recent years is going to be discussed here since there seems no direct judicial verdict to address the secondary liability of information privacy infringement to the internet service provider.

B. The Three Observations to the Preventive Measure in the Protection of Information Privacy

First of all, the best way to eliminate the issue of whether or how the information privacy shall be protected is to receive the consent of personal information provider in gathering the personal information. The legal thinking behind this is that the information privacy is a personal right and can be reduced or eliminated by way of the consent of the information provider. It can be seen from a flood of statements related to privacy policy within a variety of contract in the United States. Also, this idea of executing informed consent appears in some federal legislation and administrative regulation. For example, in HIPAA (Health Insurance Portability and Accountability Act) [40], the Congress require in this act that the entities for health care will basically get the informed consent for any disclosure of personal medical information. The new drug application for biological product and the human body test for genetic therapy will need the informed consent from the test or research subject before the approval of such application or test [41]. And, the informed consent requirement also happens in The Gramm-Leach-Bliley Act and Privacy of Consumer Financial Information, Regulation P for electronic commerce.

Secondly, beside the informed consent methodology, to put a high value of technology prevention in protecting information privacy is the other current trend of preventive measure for the information privacy infringement. The best example for the emphasis of technology security is the infrastructure for establishing technology standard in American Recovery and Reinvestment Act of 2009 [42]. Generally speaking, from Subtitle C SEC 3001-3003 in American Recovery and Reinvestment Act of 2009, Congress design to establish the Office of the National Coordinator for Health Information Technology for the purpose of setting up the technology standard, including the purpose of protection in information privacy, in order to promote the electronic medical records system.

The last observed tendency for the issue of protecting information privacy is to add the obligation of notification to who preserves the individual information when such information has been unauthorized accessed by the third party. This measurement is a fairly new legal remedy for the harm to the information privacy. For example, the detailed mechanism for how to work the requirement of notification in electronic medical records security breach is regulated in Subtitle D Part I SEC 13400 and 13402 of American Recovery and Reinvestment Act of 2009. There are also other legislations in the United States embracing the similar regulation [43].

C. One Potential Prediction to the Secondary Liability to the Internet Service Provider in the Protection of Information Privacy

Beside the above-mentioned three preventive measures in the protection of information privacy, the secondary liability to the internet service provider for information privacy invasion is potentially viable in the information age, especially in case of intelligent vehicle telematics. Until now, there is no general federal or state law to regulate the secondary liability of the internet service provider for information privacy invasion, At the same time, even there seems no direct judicial verdict to the secondary liability of the internet service provider for information privacy invasion in the United States; the article would think probably one important reason is because the court of the United States is still struggling to delineate the scope of information privacy within Internet. But this status quo is by no means to say the protection of information privacy within Internet is insignificant. On the other hand, ensuing the highly developed technology of telecommunication and the more dependency of our society to such technology, the protection of information privacy within Internet is deemed to be an important issue in the information age. Although there is no judicial decision to the secondary liability of the internet service provider for information privacy invasion at this moment, the court in the United States did make some decision with regard to the secondary liability to the internet service provider in recent years and revealed the court's leniency to the internet service provider through the following case related to the trademark infringement within Internet. In Tiffany v. Ebay [44], Tiffany file the suit for multiple causes of action against eBay. For the purpose of this discussion in this article, the focus of this case is centered on the issue of contributory infringement of trademark. The facts for this case are relatively simple. eBay offers the platform for online purchases to be concluded. Tiffany, the high-quality jewelry producer, was unhappy there are counterfeiting Tiffany jewelry circulating on eBay's online purchasing platform and filed the secondary liability litigation for trademark infringement to eBay, even eBay did have taken some kind of anti-fraud measurement for preventing the counterfeited product in its operation system. To the

issue of secondary liability to the trademark infringement, based upon the interpretation of the Supreme Court in Inwood case [45], the liability lies when "a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement." eBay definitely did not induce the trademark infringement in this case, that left the question to whether eBay was contributory liable to the trademark infringement. The court in this case discarded the "reasonable anticipation standard" as the meaning of "knows or has reason to know", instead the knowledge requirement is "a contextual and fact-specific test" judged by all the surrounding circumstances, for example the specific incident of trademark infringement, which is a higher standard than "reasonable anticipation standard". In this case, the court concluded that Tiffany could not satisfy with the high criteria for "knows or has reason to know" requirement, especially eBay has above-mentioned anti-fraud measurement in force, and eBay was not liable for contributory trademark infringement.

The Tiffany case demonstrates two kinds of policy attitude. One observation is that the court in the United States is reluctant to impute the liability to the internet service provider probably due to the concern of free flow of information. And the other observation is the court would enhance the mental requirement for the secondary liability infringer to some extent, at least near to the requirement of "willful blindness" instead of reasonable anticipation. From the description of shifting attitude to the secondary liability of the internet service provider, this judicial attitude also put the preventive measure to the protection of information privacy within Internet in the even more important position for such infrastructure.

D. The Definition of Information Privacy and the Suggested Model Building Up the Information Privacy Protection for Intelligent Vehicle Telematics

After understanding the general idea of information privacy and the tendency of protecting such legal interest in the United States, how to build the protection infrastructure of information privacy and strike the balance with other kinds of conflicting legal interest for Intelligent Vehicle Telematics operation brings the discussion to the next level. With regard to the issue of protection of information privacy in Intelligent Vehicle Telematics operation, this article would attempt to divide it into two different aspects: non-legal –binding self regulation and legal measurements for preventive or remedial purpose to the system operator. First, to the part of self regulation within the system operator, the proposed estimation in this article is that the self regulation wouldn't be able to play any significant role in striving to preserve the legal interest of information privacy before the competition in market has reached sufficient status. That is not to say the idea of self-management for the information privacy protection is not important. The statement is just to express the thinking that to establish the management system for the protection of information privacy is not easy compared with the intellectual property management system because the concept of information privacy is further developing. So, it is argued in this article, in this stage, there is no substantial meaning to emphasize the mechanism of self regulation. As to the preventive or remedial legal measurements for the protection of information privacy related to the system provider for Intelligent Vehicle Telematics, the bottom line is described as the old saying: "One stitch in time safes nine.". That leads to the indication that the preventive measurements of informed consent and technology prevention are much better than the remedial measurements (the obligation of notification, civil liability or even criminal punishment). To sum up the infrastructure for the protection of information privacy in Intelligent Vehicle Telematics, it is fairly to say in protecting information privacy in operating Intelligent Vehicle Telematics, there is a hierarchy to construct the protection, from the legal to the non-legal in general concept, from the preventive to the remedial measurement in real practice.

As to the definition of information privacy, this really means the balance of interest. In comparing the different interests to confirm the legitimacy of information privacy in the situation of Intelligent Vehicle Teleatics, the safety concern will definitely get its priority to the information privacy concern. To other comparisons between the protection of information privacy and proprietary interests of the system operator, the odds are that the information privacy will have a good chance to fight in the battlefield of balancing interests. One problematic situation of protecting information privacy within the environment of intelligent vehicle telematics is its possible interaction with the concept of protecting critical infrastructure. General speaking, under the idea of protecting critical infrastructure, the Bureau of Homeland Security can acquire and reasonably use the information related to the critical infrastructure processed by the private sector or government agencies for the purpose of anti-terrorism, which information might be under the protection of information privacy [46]. Even under the balance of interest approach, the legal interest of information privacy will be no doubt succumbed to the interest of national security if these two kinds of interest directly conflict with each other, the question is whether the environment of intelligent vehicle telematics would be treated as the critical infrastructure and to what extent of using the information contained within is reasonable [47]. The potential impact of critical infrastructure protection to information privacy protection is unknown and needs to wait and see. As the protection of information privacy is getting more and more importance in the hierarchy of different kinds of legal interest, the national security remains the strongest opposition. What is the line need to be drawn between the protection of national security and information privacy, especially in talking about the intelligent vehicle telematics environment, cannot be answered until the day comes.

V. CONCLUSION

It often times comes with the legal concern when the advanced technology seems to promise the society a better life. And this is exactly what happens to the Intelligent Vehicle Telematics. These two mainly legal concerns which are the liability both for the safety devise manufacture and the system provider, and also the protection of information privacy, under the discussion in this article, shall move toward the intensive way to go. There should be nothing wrong to be cautious about the new technology after balancing the benefits and the potential harm of such technology to reveal that it could do more harm than good to the society as a whole, especially such harm is imminent. And it is suggested in this article that the potential harm to the safety devise in Intelligent Vehicle Telematics could be a disaster for the reason of estimating human life as high-value. And also the same seriousness to the invasion of information privacy would happen especially the unauthorized use or security breach of the extensive gathering of personal information in operating Intelligent Vehicle Telematics could be fatal to the trend of enhanced protection of information privacy. For all the reasons mentioned here, this article will hold the position that the most restrictive legal responsibility under the current legal theory shall apply to these two concerns respectively. But, even the legal interest of information privacy is moving its way toward the ultimate position which is one kind of the fundamental human rights, its legal hierarchy still hasn't reached that stage yet. And the difficulties and dilemma to protect the information privacy in the information age, especially in the intelligent vehicle telematics environment, make the preventive measure to protect the information privacy get its priority and alleviate the secondary liability of the internet service provider to some extent. The influence of national security to the protection of information privacy in the environment of intelligent vehicle telematics will be the potential problem need to be resolved since there is no direct or similar judicial decision can be refered. The development of Intelligent Vehicle Telematics technology is still in its primitive stage. And it is the purpose (intention) of this article to pinpoint the legal concerns for Intelligence Vehicle Telematics in front and try to come up the positive solutions in the hope of that the discussion could, at least, have some referential value for the possible future policy making decision.

REFERENCES

[1] M. Aoyama, "Computing for the Next-Generation Automobile," *Computer*, vol.45, no. 6, pp. 32-37, 2012.

[2] F. R. Soriano, V. R. Tomás, and M. Pla-Castells, "Deploying harmonized ITS services in the framework of EasyWay project: Traffic Management Plan for corridors and networks**,"** *Euro American Conference on Telematics and Information Systems (EATIS)*, pp. 1 – 7, 2012.

[3] J. Blau, "Car Talk," 2008, Available: http://spectrum.ieee.org/green-tech/advanced-cars/car-talk. Accessed 2011 Mar. 22.

[4] W. D. Jones, "Smarter Cars? There's an App for That," 2011, Available: http://spectrum.ieee.org/green-tech/advanced-cars/smarter-cars-theres-an-app-for-that/0. Accessed 2011 April 6.

[5] M. G H. Bell, "Policy issues for the future intelligent road transport infrastructure," *IEE Proceedings - Intelligent Transport Systems*, vol. 153, no. 2, pp. 147 – 155, 2006.

[6] A. Amditis, E. Bertolazzi, M. Bimpas, F. Biral, P. Bosetti, M. D. Lio, L. Danielsson, A. Gallione, H. Lind, A. Saroldi, and A. Sjögren, "A Holistic Approach to the Integration of Safety," *IEEE Trans. on Intellignet Transportation System*, vol. 11, no. 3, pp. 554 – 566, 2010.

[7] P. Green, "Driver distraction, telematics design, and workload managers: Safety issues and solutions," *International Congress on Transportation Electronics*, pp. 165 – 180, 2004.

[8] R. N. Charette, "This Car Runs on Code," 2009, Available: http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0. Accessed 2011 Mar. 23.

[9] I. Berger, "Can You Trust Your Car?" 2002, Available: http://spectrum.ieee.org/green-tech/advanced-cars/can-you-trust-your-car/0. Accessed 2011 April 6.

[10] O. M. J. Carsten, and L. Nilsson, "Safety Assessment of Driver Assistance Systems," *European Journal of Transport and Infrastructure Research*, vol. 1, no. 3, pp. 225 – 243, 2001.

[11] M. A. Brackstone, B. Sultan, and M. McDonald, "Findings on the Approach Process Between Vehicles - Implications for Collision Warning," *Transportation Research Record – Journal of the Transportation Research Board*, vol. 1724, pp. 21 – 28, 2000.

[12] J. A. Misener, H.-S. J. Tsao, B. Song, and A. Steinfeld, "Emergence of a Cognitive Car-Following Driver Model - Application to Rear-End Crashes with a Stopped Lead Vehicle," *Transportation Research Record – Journal of the Transportation Research Board*, vol. 1724, pp. 29 – 38, 2000.

[13] A. Smiley, "Behavioral Adaptation, Safety, and Intelligent Transportation Systems," *Transportation Research Record – Journal of the Transportation Research Board*, vol. 1724, pp. 47 – 51, 2000.

[14] A. Rae, and O. Basir, "Reducing Multipath Effects in Vehicle Localization by Fusing GPS with Machine Vision," *International Conference on Information Fusion*, pp. 2099 – 2106, 2009.

[15] M. M. Trivedi, T. Gandhi, and J. McCall, "Looking-In and Looking-Out of a Vehicle: Computer-Vision-Based Enhanced Vehicle Safety," *IEEE Trans. On Intelligent Transportation Systems*, vol. 8, no. 1, pp. 108 – 120, 2007.

[16] H. Cheng, N. Zheng, X. Zhang, J. Qin, and H. van de Wetering, "Interactive Road Situation Analysis for Driver Assistance and Safety Warning Systems: Framework and Algorithms," *IEEE Trans. On Intelligent Transportation Systems*, vol. 8, no. 1, pp. 157 – 167, 2007.

[17] C. C. Huang-Fu, and Y. B. Lin, "Deriving Vehicle Speeds from Standard Statistics of Mobile Telecom Switches," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 7, pp. 3337–3341, SEPTEMBER 2012.

[18] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 742 – 755, 2011.

[19] Freeman v. Adams, 63 Cal. App. 225, 1923.

[20] Heath v. Swift Wings. Inc., 252 S.E.2d. 526, 1979.

[21] Synder v. LTG L Lufttechnische, GmbH, 955 S.W.2d 252, Tenn. 1997.

[22] V. E. Schwartz, K. Kelly, and D. F. Partlett, *Prosser, Wade and Schwartz's Torts-Cases and Materials*. West Group, 721p, 2000.

[23] Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 1960.
[24] Andrade v. Shiers, 564 So.2d 787, La. App. 1990.
[25] Golden v. Amory, 109 N.E.2d 131, 1952.
[26] "Product liability," Available: http://en.wikipedia.org/wiki/Product_liability. Accessed 2011 Mar. 23.
[27] MacPherson v. Buick Motor Co., 217 N.Y. 382, 1916.
[28] Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 1960.
[29] Greenman v. Yuba Power Products, Inc., 377 P.2d. 897, 1963.
[30] V. E. Schwartz, K. Kelly, and D. F, Partlett, *Prosser, Wade and Schwartz's Torts-Cases and Materials*. West Group. 794p, 1994.
[31] J. R. Alberts, J. Petersen, and A. L. T. Para, "Survey of Recent Developments in Indiana Product Liability Law," *Ind. L. Rev*. vol. 43, pp. 873– 917, 2010.
[32] Daly v. General Motors Corp., 575 P.2d 1162, 1978.
[33] King v. Collagen Corp., 983 F.2d 1130, 1993.
[34] Erkson v. Sears, Roebuck & Co., 841 S.W.2d 207, Mo. App. 1992.
[35] V. L. MacDougall, *Oklahoma Practice Product Liability Law*. Thomson West, vol. 8, pp. 1– 2, 2010.
[36] A. F. Amendola, "Can You Hear Me Now?: The Myths Surrounding Cell Phone Use While Driving and Connecticut's Failed Attempt at a Remedy," *Conn. L. Rev*. vol. 41, no. 1, pp. 339–379, 2008.
[37] Griswold v. Connecticut, 381 U.S. 479, 1965.
[38] S. L. Emanuel, *Constitutional Law*. Aspen Law & Business, 152p, 1998-99.
[39] Hall v. Post, 323 N.C. 259, N.C. 1988.
[40] American College of Emergency Physician, "From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine-PartI: Conceptual, Moral, and legal foundations," Available: http://www.acep.org/NR/rdonlyres/DE534243-E7D5-4A51-9827-1D95828DA45C/0/hippocrateshopaaI.pdf. Accessed 2011 Mar. 29.
[41] L. B. Andrews, M. J. Mehlman, and M. A. Rothstein, *Genetics: Ethics, Law and Policy*. West Law School. 88, 391-401p, 2002.
[42] "American Recovery and Reinvestment Act of 2009," Available: http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf. Accessed 2011 Mar. 30.
[43] T. J. Smedinghoff, "Security Breach Notification Law: Defining a New Corporate Obligation," *International securities law*, pp. 11–16, 2006. Available: http://www.wildman.com/resources/articles-pdf/Security_Breach_Notification_Law.pdf. Accessed 2011 Mar. 30.
[44] Tiffany (NJ) Inc. v. Ebay Inc. 576 F. Supp.2d 463 (S.D.N.Y.), 2008.
[45] Inwood Lab. Inc. v. Ives Lab. Inc. 456 U.S. 844, 1982.
[46] G. M. Steven, "Homeland Security Act of 2002: Critical Infrastructure Information Act," *Report for Congress* RL31763, pp. 1–16, 2008.
[47] C. Koski, "Committed to Protection? Partnership in Critical Infrastructure Protection," *Journal of Homeland Security and Emergency Management*, vol. 8, no. 1, 2011.

Fa-Chang Cheng received LL.M. degree from Golden Gate University and J.D. (Juris Doctor) degree from Ohio Northern University, U.S.A., in 1997 and 2001, respectively.

He is a full-time associate professor in Graduate Institute of Science and Technology Law of National Kaohsiung First University of Science and Technology. His major research area is focusing on the legal issues for both Telecommunication and Biotechnology.

Wen-Hsing Lai received the Ph.D. degrees in communication engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2003.

In 2006, she became an Assistant Professor of the Department of Computer and Communication Engineering, National Kaohsiung First University of Science and Technology, Taiwan. Her major research area is focusing on digital signal processing.