Journal of Multidisciplinary Research

Special Issue: The Internet of Things

Vol. 10, No. 3 Fall 2018

Journal of Multidisciplinary Research

ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Contact Information

Professor Hagai Gringarten, Ph.D., Editor-in-Chief, *Journal of Multidisciplinary Research*
c/o O'Mailia Hall, 16401 N.W. 37th Avenue, Miami Gardens, Florida 33054
Telephone +1 (305) 628-6635 E-mail: jmr@stu.edu

Journal Web Address

http://www.jmrpublication.org

Journal Indexing & Listing

Indexed in ProQuest, Cabells, EBSCO, Gale-Cengage Learning, CiteFactor, Ulrich's, de Gruyter (Germany), Elektronische Zeitschriftenbibliothek (EZB) (Germany), and European Reference Index for the Humanities and the Social Sciences (ERIH PLUS) (Norway).

Listed in *Directory of Open Access Journals*, AcademicKeys, Cision Directory, EconPapers, Gaudeamus, Google Scholar, Isis Current Bibliography, JournalSeek, Journals4Free, The Linguist List, MediaFinder, NewJour, Research Papers in Economics (RePEc), COPAC (England), CUFTS Journal Database (Canada), EconBiz (Germany), Edanz (Japan), Globethics, (Switzerland), HEC Paris Journal Finder (France), MIAR (Spain), Mir@bel (France), NSD - Norwegian Register (Norway), PhilPapers (Canada), REBIUN-CRUE (Spain), ROAD: Directory of Open Access Scholarly Resources (France), SUDOC (France), ZeitschriftenDatenBank (ZDB) (Germany), and the Open University of Hong Kong Electronic Library (Hong Kong).

Accessible via BASE-Bielefeld Academic Search Engine (Germany), and NIST Research Library (National Institute of Standards and Technology, part of the U.S. Department of Commerce).

Mission Statement

The mission of the *Journal of Multidisciplinary Research* is to promote excellence by providing a venue for academics, students, and practitioners to publish current and significant empirical and conceptual research in the arts; humanities; applied, natural, and social sciences; and other areas that tests, extends, or builds theory.

Journal of Multidisciplinary Research

Vol. 10, No. 3 Fall 2018

Contents

Articles

Reflections

Life Forward

Review

Index to Volume 10

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 3-4.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Special Issue: The Internet of Things

Guest Editorial and Preface

With this special issue, the *Journal of Multidisciplinary Research* begins a series of articles covering the multifarious repercussions of a rising new technology that goes under the name of IoT, or Internet of Things.

The special issue has a Part 1 (this issue) dedicated to the general issues of IoT (technological impact, product liability, insurance, government regulation, and national approaches in Europe and outside the U.S.A.) and a Part 2 (following in the Fall) specially dedicated to maritime automation. A Part 3 is planned for 2019 about the legal and commercial issues raised by "3-D Printing," also known as "remote manufacturing."

The inspiration for this endeavor came from a seminar organized in the Spring of 2017 at Washington, D.C., for the American Bar Association by the then-Committee Chair Andrew Danas, to whom go our thanks and credit.

The conceiving and making of this Series dedicated to Interdisciplinary Issues of IoT dates back to old personal roots.

Artificial Intelligence reached consumers with a computer program by the name of COBOL,[1] designed in 1959.[2] It was on the shelves of computer stores when I was beginning my second law-student life at the University of Miami in 1984. The possibility of creating my own A.I. (artificial intelligence) companion was irresistible. I tried to automate many chores of research and production of essays.

At that time, however, I had only an Apple II c, 5" floppy, too small for creating anything of practical value. I stopped that vein not for lack of interest but for lack of readily available technology. The A.I "bug," however, remained dormant in me, until I had a faint awakening by Professor Martin Davies[3] about 35 years later.

Speaking at an Admiralty Law Institute at Tulane University, Professor Davies gave a presentation on "3 D Printing," an issue of which I then was totally ignorant. It looked like

[1] Common Business-Oriented Language

[2] For a history and description of the program, see https://en.wikipedia.org/wiki/COBOL#COBOL-85

[3] Admiralty Law Institute, Professor of Maritime Law and Director, Maritime Law Center, University of Tulane School of Law.

science fiction, but the propositions were intriguing. Professor Davies suggested that if ever 3 D Printing were to have large commercial-scale implementation, the world of transportation (theme of that ALI) would dramatically change.

Again, my interest remained dormant a few years, until Andrew Danas (then Chair of the ABA International Transportation Committee) called me to join a presentation he was preparing on "Disruptive Technologies" (read: IoT).[4] My task was to do a study on shipping automation and on "crew-less" ships in particular.

What I found conducting that study definitely shook me out of my torpor. The amount of information on the technology that was developing was shocking, both in substance and quantity. Countless conventions were taking shape worldwide, automatic cars and trucks were on the road (I even learned that automated trucks were delivering my can of Coors beer), machines answered telephone calls with voices so human as to include nuances of personal comments, and countless trivial daily activities were taking place through wireless automated links). I understood what Andrew Danas meant by "Disruptive Technologies," "Shared Economy" and "IoT" (till then a mysterious acronym).

It was then that the project of a dedicated publication was born, and this journal is its ideal home.

The issues and involvements that IoT may and will create are by definition "multidisciplinary": technological first of all, but also commercial, legal, financial, political, and last but not least, ethical.

Another motive for launching this enterprise is that, against the enormous volume of information, the scholarly articles in law reviews are relatively scarce, while we find an abundance of blogs from specialized corporations, Law Firms, and even governmental bodies. This is not surprising because litigation of IoT matters is still in a deep infancy; therefore, any meaningful writing could be only on speculation of possible future legal problems, and only conjectures in most cases.

The goal of this special issue of our journal is to offer a Forum where the issues could be gathered, addressed, and developed in a channeled, organic and orderly form, with the professional language and research tools used all contributors of any kind use: tech experts, lawyers, insurers, regulators, anyone who is part of this, still unknown, "shared economy."

This issue (Part 1) is introductory, aimed at giving a bird's eye view of the IoT issues that have gathered most perception and attention: general consequences of automation on social life at large, product liability and cyber risks, insurance, and government regulation in the USA and abroad.

A second issue (Part 2) will follow, dedicated to the specific and specialized field of Autonomous Shipping. A third issue is in the preparation stage, and it will cover issues of "3D" Remote Manufacturing. I hope you will enjoy.

Attilio M. Costabel, Esq.
Guest Editor

[4] Andrew Danas is a Partner with Grove, Jaskiewicz and Cobert LLP, in Washington, D.C., and Co-Chair of the International Transportation Committee of the American Bar Association Section on International Law.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 5.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Featured Artwork

"Stolen Girls…Stolen Dreams"

"Blindsided" by Emily Whitsett

"No Returns" by Julian Rush

"Behind Every Smile" by Wen Cheng

In this issue, the *Journal of Multidisciplinary Research* (JMR) features very special artwork – the winners of "Stolen Girls…Stolen Dreams," the Soroptimist International of Davie Human Trafficking Poster Contest Awards 2018.

Soroptimist International of Davie (SID), Florida, is a 501 (c)(3) organization dedicated to improving the lives of women and girls. Organized in 1983, the Davie club is part of "an international volunteer service organization for business and professional women who work to improve the lives of women and girls in local communities and throughout the world" (SID, 2018) with programs worldwide. In the past 30 years, it has supported a variety of service projects, gifting more than $250,000 in awards to local women and girls, with additional in-kind resources and donations.

In 2014, SID established the "Stolen Girls…Stolen Dreams" poster contest as part of its human trafficking awareness outreach work.

In cooperation with SID, and with permission of the artists and their parents, the JMR is pleased to present the artwork of the 2018 contest winners:

Award	*Title*	*Artist*	*Affiliation*
First Place	"Blindsided"	Emily Whitsett	Western High School
Second Place	"No Returns"	Julian Rush	College Academy of Broward County
Third Place	"Behind Every Smile"	Wen Cheng	Western High School

We are glad to have you, the reader, join us in celebrating the important work of these young artists. – *The Editors*

Reference

Soroptimist International of Davie. (2018). About us. Retrieved from http://www.sidavie.org/about

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 7-21.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

The Internet of Things: The Future was Yesterday

Attilio M. Costabel

Abstract

This article supplies a review of some of the major regulatory and business developments in the area of IoT automation in Europe and beyond. After a short introduction on the theme that inspired this series, Part 1 supplies a note on the meaning and history of the term "Internet of Things." Part 2 deals with the policies and aspirations that are unfolding in Europe and some works in progress in the European Union, such as industry alliances and grants, platforms, intelligent transportation system, digital single market, "Horizon 20 20" and others. Part 2 ends with a review of the EU's legislative works in progress and Commissions' Recommendations about regulation of Artificial Intelligence, with a special comment on a Recommendation to create a special "person" status for certain robots capable of independent learning and independent decisions. Part 3 deals with the specific subject of automated vehicles seen through a report issued by the global audit Firm KPMG on the progress of studies and regulations of automated vehicles worldwide (the Report is named AVRI - "Automated Vehicles Readiness Index"). The rankings of the index are limited to 20 Countries and are based on factors of policy and legislation, technology and innovation, infrastructure and consumer acceptance. Following the "Index", this part examines the status of selected European Countries (United Kingdom, Germany, France, Netherlands and Sweden, ranked respectively #5, 6, 13, 1 and 4) and beyond Europe the status of China (#15) and of surprising Singapore, ranked #2. The review closes with a mention of Israel, not ranked in the range of 20, yet deserving mention for its deep involvement and progress in IoT and vehicular automation. At the end, the article supplies two Appendixes: the 20-Country AVRI Index and a chart of Israeli technology.

Keywords: Internet of Things, IOT, alliances, platforms, digital single market, artificial intelligence, automated vehicles

Part 1: IOT – The Term and History

There is general consensus that Kevin Ashton coined the term IoT in 1999 during a presentation he made at Procter & Gamble,[5] though Prof. Doctor Henning Kagermann is also

[5] See, among many others: https://iot-analytics.com/internet-of-things-definition/; and https://datafloq.com/read/where-does-the-internet-of-things-come-from/524

credited with creation of the IoT concept for his role in forging strategic projects such as Industry 4.0, Smart Services and Autonomous systems.[6]

A recent blog[7] has an interesting historical timeline, suggesting that IoT began, as concept, as early as 1926 with a prediction by none less than Nikola Tesla. In 1950, Alan Turing questioned whether machines could think,8 then the blog gives 1969 as the official date of birth of Internet with the first nodes by UCLA and Stanford Universities. The first "connected devices" came in 1989 with the "House of the Future" in the Netherlands, and in 1990 appeared the first "connected toaster" by Sunbeam, followed by a smart refrigerator in year 2000.[9]

The United Nations mentioned IoT in 2005, and a first Conference on IoT took place in Zurich in 2008.[10]

The "Internet Protocol version 6" became an Internet standard July 14, 2017.[11]

Part 2: Europe

To give a full rendering of all that is developing in Europe is outside the scope of this publication. A whole book would be necessary, maybe a library.

Automated cars are covered by Directive 2007/46/EC,[12] which has no technical requirements, and by ECE Regulation 79, which has requirements for steering functions.[13]

For automated ships, there is a collaborative research project under the name of MUNIN (Maritime Unmanned Navigation through Intelligence in Networks), which the European Commissions co-fund, with the aims of developing concepts and rules for autonomous ships, with the definition of "vessels primarily guided by automated on-board decision systems but controlled by a remote operator in a shore side control station."[14]

Both topics are too large to be covered properly in this article. Autonomous ships will be covered in Part 2 of this Special Issue (forthcoming).

IoT in Europe

For at least ten years, the European Union (EU) Commission, Council, Parliament and work Groups of the same and other Agencies produced an overwhelming volume of initiatives, studies, resolutions, and recommendations.

Here, few key products will suffice.

In the EU, we see a parallel unfolding of public and private activities and researches. EU Authorities are working in many directions: the promotion of synergies and alliances of private enterprises, the funding of grants for research and development programs, the development of an

[6] https://www.linkedin.com/pulse/digital-transformation-manufacturing-industries-prof-dr-gaddam/

[7] https://datafloq.com/read/where-does-the-internet-of-things-come-from/524

[8] A.M. Turing, COMPUTING MACHINERY AND INTELLIGENCE, http://cogprints.org/499/1/turing.html

[9] Supra at Fn 3.

[10] Ibid.

[11] Ibid.

[12] https://ec.europa.eu/growth/sectors/automotive/legislation/motor-vehicles-trailers/directive-2007-46-ec_en

[13] Found at http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/r079r2e.pdf

[14] http://www.unmanned-ship.org/munin/

Intelligent Transport System, the creation of a "Digital Single Market," support of research, initiatives, and implementation: the so-called "Horizon 20 20" and regulation of Robotics and Artificial Intelligence.

Industry Alliances and Grants

- **AIOTI (Alliance for Internet of Things Innovation)**

The EU Commission launched the Alliance in 2015 in order to create a platform for the widest cross-exchange of data among the European industries.[15] AIOTI is incorporated as a Belgian international non-profit association, with registered office at 1000 Brussels (Belgium) de Meeûssquare 23. Its mission is, among other things, collaborating with the European Commission for the implementation and execution of European framework programs for research and innovation; collaborating and coordinating with other European innovation platforms and industry organizations that have IoT related topics; identifying and attempting to resolve market obstacles for IoT deployment; organizing and facilitating matchmaking events and joint ventures; collecting and raising the financial resources necessary. The Members are a wide cross-representation of industries[16] and of sectors.[17] Some of the most important Members are Alcatel, Bosch, Cisco, Hildebrand, IBM, Intel, Landis+Gyr, Nokia, ON Semiconductor, Orange, OSRAM, Philips, Samsung, Schneider Electric, Siemens, NXP Semiconductors, STMicroelectronics, Telecom Italia, Telefonica, Telit, Thales, Vodafone, Volvo), and start-ups (SIGFOX).

- **EU Platforms**

  - ARTEMIS Industry Association – Advanced Research & Technology for Embedded Intelligence and Systems.[18]
  - **ECSEL Joint Undertaking – Electronic components and systems for European leadership[19]**
  - **EPoSS – The European Technology Platform on Smart Systems Integration.[20]**
  - ERTRAC – European Road Transport Research Advisory Council.[21]
  - Smart Grids European Technology Platform.[22]
  - Fuel Cells and Hydrogen Joint Undertaking.[23]

[15] https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti

[16] nanoelectronics/semiconductor companies, Telecom companies, Network operators, Platform Providers (IoT/Cloud), Security, and Service providers.

[17] Energy, utilities, automotive, mobility, lighting, buildings, manufacturing, healthcare, supply chains, cities, etc.

[18] ARTEMIS Industry Association is the association for actors in Embedded & Cyber-Physical Systems within Europe. As private partner, the association represents its members – industry, SMEs, universities, and research institutes – in ECSEL Joint Undertakings. https://www.earpa.eu/earpa/40/artemis_ia.html

[19] https://www.earpa.eu/earpa/56/ecsel_ju.html

[20] https://www.earpa.eu/earpa/37/eposs.html

[21] https://www.earpa.eu/earpa/36/ertrac.html

[22] https://www.earpa.eu/earpa/39/etp_smartgrids.html

- iMobility Forum.[24]

- **Intelligent Transport System**

With Directive 2010/40/EU of 7 July 2010, [25] the European Parliament adopted a new legal framework to address innovative transport technologies and to coordinate implementation of Intelligent Transport System (ITS) in Europe.

The Directive gave the European Commission a seven year term to adopt functional, technical, and organizational specifications for ITS solutions with priority to traffic and travel information, e-Call emergency system, and intelligent truck parking.[26]

Following these guidelines, the Commission took a major step on 16 December 2008 by adopting an Action Plan.[27] The Action Plan suggested six targeted measures and proposals:

Action Area 1: optimal use of road and traffic data;
Action Area 2: Continuity of traffic and freight management ITS services on European transport corridors;
Action Area 3: Road safety and security;
Action Area 4: Integration of the vehicle into the transport infrastructure;
Action Area 5: Data security and protection, and liability issues; and
Action Area 6: European ITS cooperation and coordination.

Five cooperating Directorates General support the initiative: DG Mobility and Transport (lead); DG Communications Networks, Content, & Technology; DG Research & Innovation; DG Enterprise and Industry; and, DG Climate Action.[28]

Numerous proposals, Directives, Working Programmes, and Delegated Acts, were passed in the wake of Directive 2010/40/EU.[29]

In February 2018, the European Parliamentary Research Service (EPRS) published a study by Tatjana Evas[30] titled, "The European added value of a common EU approach to liability rules and insurance for connected and autonomous vehicles."[31]

The study contains two attachments of studies of legal and socio-economic analysis.[32]

---

[23] https://www.earpa.eu/earpa/38/fuel_cells_and_hydrogen_ju.html
[24] https://www.earpa.eu/earpa/41/imobility_forum.html
[25] http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32010L0040
[26] https://ec.europa.eu/transport/themes/its/road/action_plan_en
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008DC0886
[28] Supra, at fn. 4.
[29] A list is available at https://ec.europa.eu/transport/themes/its/road/action_plan_en
[30] Tatjana Evas, European Parliamentary Research Service, Impact Assessment and European Added Value Directorate, European Added Value Unit, European Parliament, B-1047 Brussels. To contact the unit, please e-mail EPRS-EuropeanAddedValue@ep.europa.eu
[31] The abstract reads, "The findings of this European added value assessment (EAVA) suggest that it is necessary to revise the current legislative EU framework for liability rules and insurance for connected and autonomous vehicles. Not only would revision ensure legal coherence and better safeguarding of consumers rights, but it would also be likely to generate economic added value. It is argued that accelerating the adoption curve of driverless or autonomous vehicles (AVs) by five years has the economic potential to generate European added value worth approximately €148 billion" (emphasis supplied).

- **Digital Single Market**

On May 6, 2015, the EU omission adopted a strategy known under the name of "Digital Single Market" (COM 2015 192) and delivered 16 specific initiatives by January 2017.[33] The European Parliament and the Council currently are discussing legislative proposals.

The strategy runs on what the Commission called "three pillars":

1. Access: better access for consumers and businesses to digital goods and services across Europe;
2. Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish; and
3. Economy & Society: maximising the growth potential of the digital economy.

In April 2016, the Commission then launched the Digitizing European Industry initiative (DEI), based on "five pillars"[34]:

1. European platform of national initiatives on digitizing industry.[35]
2. Digital innovations for all: Digital Innovation Hubs.[36]
3. Strengthening leadership through partnerships and industrial platforms.[37]
4. A regulatory framework fit for the digital age.[38]
5. Preparing Europeans for the digital future.[39]

[32] Annex I: Legal analysis of the EU common approach on the liability rules and insurance related to connected and autonomous vehicles, by Dr E.F.D. Engelhard and R.W. de Bruin, LL.M., within the Utrecht Centre for Accountability and Liability Law. Annex II: Socio-economic analysis of the EU common approach on the liability rules and insurance related to connected and autonomous vehicles by Charlene Rohr and Fay Dunkerley at RAND Europe and by Professor David Howarth from the University of Cambridge.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192

[34] https://ec.europa.eu/digital-single-market/en/pillars-digitising-european-industry-initiative

[35] This EU coordination forum brings together all Member States to ensure coherence and collective steer. The goal is to build a critical mass of initiatives and investments for digitising industry, and to ensure the commitment of Member States, regions and private sector to achieve the DEI goals.

[36] Digital Innovation Hubs (DIHs) are one-stop-shops where companies –especially SMEs, startups and mid-caps– can get help to improve their business, production processes, products and services by means of digital technology. One of the key DEI priorities is to support a strong network of DIHs to ensure that every company in Europe can take advantage of digital opportunities.

[37] To reinforce the EU's competitiveness in digital technologies, the DEIinitiative supports both the development of digital industrial platforms and large-scale piloting and Public-Private Partnerships (PPPs) that provide the digital technology building blocks of the future.

[38] A digital-friendly regulatory framework is important for the EU's industry and economy to strive. Within the Digital Single Market strategy, the European Commission has already proposed several measures to update regulations in key fields for industry such as cybersecurity and free flow of data.

[39] To make the most of the digital transformation we must ensure that all Europeans are ready for these changes. Adapting the workforce and our education and learning systems, together with major investments in reskilling citizens are needed. European initiatives such as the digital skill and jobs coalition and the digital opportunity scheme can help to bridge the gap.

For useful links about Digitizing European Industry, see https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry.

For a Mid-Term review of the progress of DEI, see Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Brussels, 10-5-2017, COM(2017) 228 final.[40]

- **Horizon 20 20**

Horizon 20 20 is an EU Research and Innovation programme, part of the EU Framework Programme for Research & Innovation, endowed with nearly €80 billions of funding over seven years (2014 to 2020).[41]

To qualify for standard research projects, a consortium of at least three legal entities established in an EU Member State or an Associated Country must make an application. For other programmes,[42] the condition for participation is one legal entity established in a Member State or in an Associated Country.[43]

The programme finances emerging technologies, infrastructure, and industrial technologies; gives access to risk financing; supports research in the areas of medical, biological, energy, mobility, climate and environment, social sciences and humanities, and nuclear research.

These goals are pursued by funding, grants, coordination and support, training, all under fast track, audits, and single funding rates for all beneficiaries.

Horizon 2020 is open to the participation of researchers from across the world.

For more information, you can visit https://ec.europa.eu/programmes/horizon 2020/what-horizon-2020.

- **Robotics and Artificial Intelligence**

This is by far the most interesting area of the EU's regulations and regulatory studies because it addresses legal issues of robotics.

The radically innovative developments in robotics and artificial intelligence prompted the EU Parliament to launch studies for recommendations of thorough review of civil law rules on robots and robotics.

The Committee on Legal Affairs and the JURI Committee set up a working group in 2015 with the aim of drawing up "European" civil law rules in the area of robotics. The study was commissioned to Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs – Legal Affairs.

[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228

[41] http://ec.europa.eu/programmes/horizon2020/en/news/horizon-2020-brief-eu-framework-programme-research-innovation

[42] E.g., European Research Council (ERC), SME Instrument, the co-funding of national or public sector calls or programmes, coordination and support, training, and mobility.

[43] Supra fn. 13.

On 31 May 2016, the study group delivered a draft report setting out a series of recommendations, including critical comments on a motion for a European Parliament resolution, and in October of the same year, the group completed its manuscript.[44]

The study is a comprehensive review of the definitions of robots ("autonomous" and "smart"), of their "consciousness," and of their "ethical" framework.

The most interesting part is on the "Incongruity of establishing robots as liable legal persons" and on "Liability for damages caused by an autonomous robot."[45]

A tentative draft of motion for Resolution contained the proposal to create

> *a new category of individual*, specifically for robots: *electronic persons*. Paragraph 31(f) of that draft called upon the European Commission to explore the legal consequences of creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations, including that of making good any damage they may cause [to third parties], and applying electronic personality to cases where robots make smart autonomous decisions or otherwise interact with third parties.[46] (emphasis supplied)

Notice this chapter of the study was under the title of "Issue Surrounding Liability in Robotics." The study concluded that, "When considering civil law in robotics, we should disregard the idea of autonomous robots having a legal personality, for the idea is as unhelpful as it is inappropriate."[47]

Notwithstanding the conclusions of the study, the Committee on Legal Affairs, on 27 January 2017, issued a Report with recommendations to the Commission on Civil Law Rules on Robotics, insisting on the recommendation of making a new legal status for robots.

Paragraph 59 of the report reads as follows:

> 59. Calls on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore, analyze and consider the implications of all possible legal solutions, such as:
> …
> f) creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently. [48]

[44] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

[45] Id. at 3.1 and 3.2.

[46] Ibid.

[47] Ibid.

[48] 2015/2103(INL), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN#title1

The reasons in the Report are deeply articulated. At Point Z on Liability, the Committee opens with the remark that today's robots are capable of quasi-independent decisions, having certain autonomous and cognitive features,[49] and "the more autonomous robots are, the less they can be considered to be simple tools in the hands of other actors (such as the manufacturer, the operator, the owner, the user, etc.)."[50]

From this premise, the Committee suggests that the ordinary rules of liability are not sufficient and that fresh rules should undergo study for responsibility for the acts and omissions of robots where the cause cannot be traced back to a specific human actor.[51]

The Report continues suggesting that where the robot is capable of taking autonomous decisions, the traditional liability rules would not make it possible to identify the party responsible for compensation.[52] The Report also argues that, today, robots may also be capable of negotiating contractual terms, thus, also that civil contract rules are inadequate for robots.

The "Whereas" of the Report concludes that robots are "equipped with adaptive and learning abilities entailing a certain degree of unpredictability in their behavior, since those robots would autonomously learn from their own variable experience and interact with their environment in a unique and unforeseeable manner," and this is the foundation for proposing the creation of a "personality" of robots.[53]

If the recommendation of the Report is followed, it could become a Directive that is a model of law for the whole of Europe. However, dissent and opposition is brewing.

The Blog "Politico" recently reported that 156 experts from 14 countries have written a letter to the EU Commission warning against adoption of the Report's proposal.[54] The doors to a paradise of legal debate are now wide open, even if, once again, only on a background of speculation.

There are many details here that have not been yet addressed. For example, even assuming that a robot could be held "personally" liable for a tort, how would the traditional civil remedies follow?

If robots have to compensate victims, they must have money to give, but how would robots acquire and keep money?

Could they open bank accounts?

They will have to be given a Social Security Number, or an ITIN. Will they have, then, to file a Tax Return?

Or, if the robot is destitute, could the rule of the ancient Roman Empire be used: The tortfeasor would work for the victim as a slave?

If the civil tort is at the same time a crime or misdemeanor, how could a *mens rea* be ascertained?

Could a robot be called for jury duty? How would it (he or she?) be evaluated in a voir dire?

While we hear many arguments about robots' liability, little is heard about rights of "personalized" robots. Will there be "robot-human rights"? Anti-discrimination protections? In case of damages or defects of the robot's hardware and software that could not be repaired,

[49] Id. at Z.
[50] Id. at Z, AB.
[51] Ibid.
[52] Id. at Z, AF.
[53] Id. at Z, AI.
[54] https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/

would there be an RDA (Robot with Disability Act)? Or could a robot be euthanized? Would there be an Obama Care Act for ailing robots?

Conversely, could the unique capabilities of a robot cause discrimination toward humans in the workplace?

Part 3: IoT Specialty

Automated Vehicles

The Vienna Convention of November 8, 1968 on Road Traffic[55] has 67 contracting parties worldwide, with notable absence, among others, of the United States and China.[56]

The global audit Firm KPMG has issued a 60 pages "index" on the progress of studies and regulations of automated vehicles worldwide ("Automated Vehicles Readiness Index" AVRI).[57] The rankings are based on factors of policy and legislation, technology and innovation, infrastructure and consumer acceptance.

The chart produced by KPMG[58] supplies valuable details for analysis. Next to the total score per Nation, the chart has four columns: Policy and Legislation; Technology and Innovation; Infrastructure; Consumer Acceptance. Each column, in turn, has two sub-columns, one for the score and one for the resulting rank.

Using this display of data, it is interesting to compare the rankings with an eye to the breakdown. For example, United States (#3) and Sweden (#4) have almost identical Total Score (24.75 vs. 24.73) but Sweden has a slight lead in Policy and Legislation (6.83 vs 6.38 of the USA) and in Infrastructure (6.04 vs. 5.84 of the USA), while USA has a lead in Technology and Innovation (6.97 vs. 6.44 of Sweden). Consumer Acceptance is again almost identical (USA 5.56 vs. Sweden 5.41). A chart of the first 20 Nations is available at AVRI, page 3.[59]

Europe

Virtually all European nations are part to the Convention and have their own domestic Road Regulations. Regulations of automated vehicles have been introduced in some Nations by statutes, guidelines or Bills under work in progress.

United Kingdom

The United Kingdom has ratified the Vienna Convention only very recently, March 28, 2018. A Bill introduced in the British Legislature in 2016 under the original name of Modern Transport Bill, then renamed Vehicle Technology and Aviation Bill and finally Automated and

[55] https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&lang=en

[56] For a list of countries, see http://www.unece.org/fileadmin/DAM/trans/conventn/CP_Vienna_convention.pdf

[57] https://home.kpmg.com/xx/en/home/insights/2018/01/2018-autonomous-vehicles-readiness-index.html

[58] See Appendix 1 to this article.

[59] Supra at Fn. 3.

Electric Vehicles Bill passed the Commons on January 29, 2018, then the House of Lords and got Royal Assent on July 19, 2018.

The Automated and Electric Vehicles Act 2018 is now an act of Parliament, that is a law of the United Kingdom.[60]

The Act is in two Parts. Part 1 deals with automated vehicles in eight Sections. Section 2 sets rules on liability of insurers, holding the insurer or the owner of the car responsible for damages suffered as consequence of accidents caused by the automated car, depending on whether the vehicle is insured or not.

Sections three to five have rules on contributory negligence, unauthorized alterations or failure to update software and subrogation rights of the insurer against persons responsible for accidents, with special reference to the car manufacturers and software producers.

The Association of British Insurers has posted interesting comments, expressing satisfaction for the adoption of the regulatory framework proposed by the ABI.[61] Also, ABI expects automatic vehicles to appear on English roads from 2021, but suggests not to have high expectations. "*The cars will not be able to drive themselves, and the person behind the steering wheel must be prepared to take back control of the car at any time when the vehicle is operating in automated mode. Fully driverless pods used for public transport may start appearing in the next 10 years, while driverless cars for consumers may be further in the future*."[62]

ABI also noted that questions remain about availability of post-accident data and the development of the relative technology that would make it possible for insurers to determine the causes of the accident.[63] The UK ranks 5th in the AVRI Index.

Germany

Germany is a party to the Vienna Convention on Road Traffic since August 3, 1978, with amendments in force December 7, 2016. Road traffic is governed by the Federal Road Traffic Act.[64] A so called "AV" Bill enacted on June 21, 2017 authorizes the use of automated vehicles, introducing few additions to the Road Traffic Act. Among the most interesting: the requirement that each automated vehicle be equipped with a "black box" that would identify the control and use of the vehicle. Also, the driver, if present in the vehicle, is allowed to divert attention for an adequate time (a detail that will require legal interpretation).[65]

In June 2017 the Ethics Commission, upon appointment by the Federal Minister of Transport and Digital Infrastructure, delivered a Report on Ethical rules for automated and

[60] Automated and Electric Vehicles Act 2018 - 2018 CHAPTER 18. See the legislative report at https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles.html and the text of the Act at http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted/data.html http://www.legislation.gov.uk/ukpga/2018/18/enacted/data.pdf

[61] https://www.abi.org.uk/news/blog-articles/2018/07/automated-and-electric-vehicles-bill-legislating-for-the-future-of-driving/

[62] Id.

[63] Ibid.

[64] Strassenverkehrsgesetz, "StVG," see Wikipedia, https://de.wikipedia.org/wiki/Stra%C3%9Fenverkehrsgesetz

[65] See 23 Jun 2017 Article, White & Case Technology Newsflash, Dr. Markus Burianski Christian M. Theissen, https://www.whitecase.com/publications/article/germany-permits-automated-vehicles

connected vehicular traffic. Several ethics rules on the subject are under development in Germany.[66] Germany ranks 6th in the AVRI index.

France

Experimentation of automated vehicles in France lags behind. At present, only few companies are conducting trials and only in restricted areas. A legislative framework is under work and is expected to appear in 2019, while a regulatory framework may not be ready until 2022.[67] France ranks 15th in the AVRI Index.

Netherlands

The Netherlands ranks first in the AVI Index. The Delft University of Technology issued a 56 pages study on scenarios for the years 2030 and 2050, with the following conclusions: "In conclusion, our study suggests that fully automated vehicles will likely be a reality between 2025 and 2045 and are expected to have significant implications for mobility and planning policies in the Netherlands. The pace of development and subsequent implications largely depend on technological evolution, policies and customers' attitude."[68]

Sweden

Sweden ranks fourth in the AVRI Index, though with a score very close to the one of the 3rd ranking United States, thanks to: "highest number of AV company headquarters by head of population, a strong showing on AV investments…and one of the highest ratings from the World Economic Forum for availability of the latest technology. Swedish-based (although Chinese-owned) vehicle maker Volvo has undertaken several AV initiatives, including a US$300 million joint-venture with Uber; a safety initiative also involving Autoliv and Ericsson; and research giving self-driving cars to real users on a pre-selected route in Gothenburg."[69] For more information on Sweden, see https://www.forbes.com/sites/heatherfarmbrough/2018/01/31/ugly-but-useful-stockholm-introduces-driverless-busses/#e76e38c60f44

And Beyond…

China

China ranks 16 in the AVRI but shows signs of aggressive developments. The news agency Reuter posted that the Chinese Government is considering the adoption of some of the

[66] See https://www.roboticsbusinessreview.com/unmanned/germany-creates-ethics-rules-autonomous-vehicles/

[67] https://www.autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials

[68] https://www.bna.nl/wp-content/uploads/2016/02/Development-of-automated-vehicles-in-the-Netherlands-TU-Delft.pdf

[69] https://home.kpmg.com/xx/en/home/insights/2018/01/2018-autonomous-vehicles-readiness-index.html at page 19.

German rules for self-driving cars, for the advanced level of technology reached by Germany and for the benefits of a synergy in a highly technical area.[70]

Two newsletters available online report that: "On December 15, 2017, three government agencies of the Beijing Municipality (i.e. the Beijing Municipal Commission of Transport, the Beijing Traffic Management Bureau and the Beijing Municipal Commission of Economy and Information Technology) jointly released the Guiding Opinions of the Beijing Municipality on Accelerating the Work of Road Tests for Autonomous Vehicles (for Trial Implementation) ("Guiding Opinions") and the Detailed Implementation Rules of the Beijing Municipality for the Administration of the Road Tests of Autonomous Vehicles (for Trial Implementation) ("Implementation Rules"). Although the Guiding Opinions and the Implementation Rules are applicable in Beijing only, they are the very first regulations dealing with road tests of autonomous vehicles in China."[71]

Singapore

Last, but not least, Singapore ranks number two in the AVRI Index, less than two point below number one Netherlands.

In a post by Bloomberg,[72] we read that in November 2017, Singapore has even built a 2-hectare mini town for test and actual use of autonomous vehicles, with intersections, traffic lights, bus stops, and pedestrian crossings, all with the same specifications for the public roads.

From a mini hill, sensors check how vehicles perform; mock skyscrapers mimic the radio interference from tall buildings and a rain machine simulates the island's frequent tropical rains. The Singapore government is expected to draft regulations by the second half of 2018.

More than 10 companies are testing vehicles at a facility of the Nanyang Technological University in the west of Singapore, and two buses from Volvo AB are expected to join early 2019.

Looking back at the PKMG Index, it is worth noting that Singapore (#2) overcomes the USA (#3) in all but Technology (USA 6.97 vs. 4.26 Singapore).[73]

A Word About the Great Absent: ISRAEL

The PKMG Index does not list Israel in the 20 Nations chart, and it is proper to wonder why, given that the Nation does not appear to be second to none when it comes to technology.

Israel is the home of Mobileye Vision Technology Ltd, a multinational recently acquired by the Intel Group for 15.3 Billion Dollars. Headquartered in Jerusalem and with offices in New

---

[70] https://www.reuters.com/article/us-autos-autonomous-germany-china/china-may-adopt-some-of-germanys-law-on-self-driving-cars-expert-idUSKCN1GR2TJ

[71] See https://globalcompliancenews.com/china-autonomous-vehicles-20180122/; and https://www.bakermckenzie.com/en/insight/.../2018/01/beijing-autonomous-vehicles

The newsletters also supply information on the key definitions found in the Guiding Opinions, namely of Autonomous Vehicles, driving Functions, Autonomous Driving System. The newsletters also inform about the designated Authorities, the requirements for application, the test of the AV, the test of the drivers, the Administration competent for the tests and treatment of accidents during trials.

[72] https://www.bloomberg.com/news/features/2018-06-04/singapore-built-a-town-to-test-autonomous-self-driving-vehicles

[73] Singapore vs. USA: Policy and Legislation: 8.49 vs. 6.38; Infrastructure: 6.72 vs. 5.84; Consumer Acceptance: 6.63 vs. 5.56.

York, Shanghai, Tokyo and Dusseldorf, Mobileye, as Intel subsidiary, is developing the so called ADAS (Advanced Driver-Assistance Systems).[74]

Also, Audi entered into a joint venture with a local autonomous vehicle simulation platform provider Cognata Ltd,[75] and Israeli autonomous technology developer, Innoviz Technologies Ltd. is entering China's car market.[76]

A recent blog titled "Israel, a land flowing with AI and autonomous cars" has reported intense exchanges with groups of American investors, posting a chart of the areas of technology that Israel is pursuing.[77]

The Government is also funding projects for smart transport,[78] and the expertise in the area of defense is not to be forgotten.[79]

Conclusion

A whole new world of the future is unfolding while we struggle with our old and entrenched rules and legal concepts. All that we have published in this journal issue looks to us as something that still has to come, but invisibly it is unfolding, and since some time.

The future actually happened yesterday, when exactly we do not know.

Perhaps one day, some Archeologist of IoT, digging through the fossils of Artificial Intelligence, will be able to ascertain an approximate date when the future began its evolution.

[74] https://www.timesofisrael.com/mobileye-autonomous-vehicle-runs-red-light-in-jerusalem/; https://en.wikipedia.org/wiki/Mobileye

[75] https://www.reuters.com/article/us-cognata-audi/audi-partners-with-israels-autonomous-vehicle-simulation-startup-cognata-idUSKBN1JM15X

[76] https://techcrunch.com/2018/06/06/israeli-autonomous-technology-developer-innoviz-is-entering-chinas-car-market/

[77] https://robohub.org/israel-a-land-flowing-with-ai-and-autonomous-cars/ See chart at Appendix 2.

[78] https://en.globes.co.il/en/article-govt-to-fund-autonomous-car-smart-transport-projects-1001240400

[79] https://www.reuters.com/article/us-autos-tech-israel-insight/israels-defense-expertise-drives-tech-boom-for-autonomous-cars-idUSKCN1IO0S8

Appendix 1

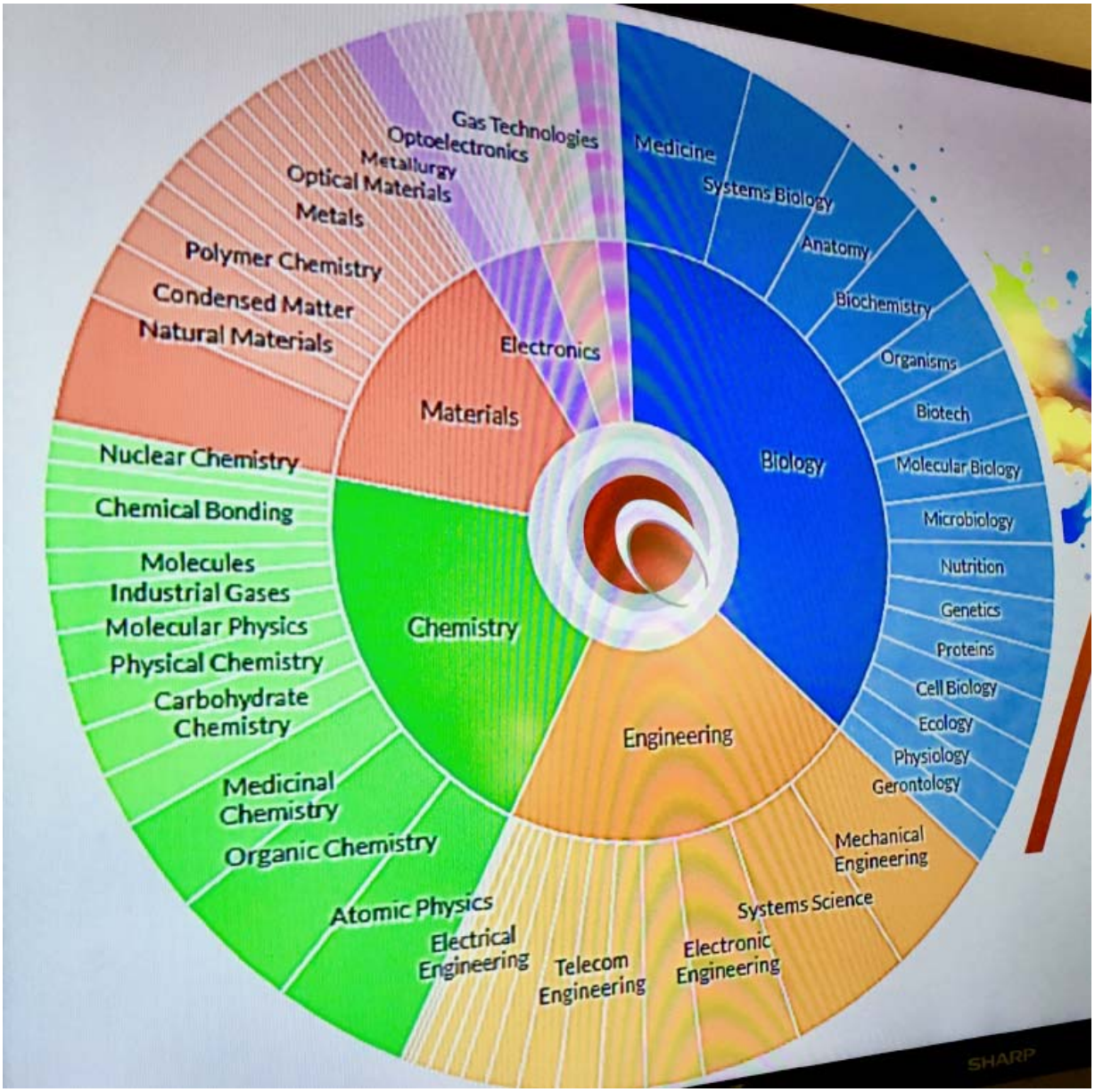
KPMG Index Results

Overall rank	Country	Total score	Policy and legislation		Technology & innovation		Infrastructure		Consumer acceptance	
			Rank	Score	Rank	Score	Rank	Score	Rank	Score
1	The Netherlands	27.73	3	7.89	4	5.46	1	7.89	2	6.49
2	Singapore	26.08	1	8.49	8	4.26	2	6.72	1	6.63
3	United States	24.75	10	6.38	1	6.97	7	5.84	4	5.56
4	Sweden	24.73	8	6.83	2	6.44	6	6.04	6	5.41
5	United Kingdom	23.99	4	7.55	5	5.28	10	5.31	3	5.84
6	Germany	22.74	5	7.33	3	6.15	12	5.17	12	4.09
7	Canada	22.61	7	7.12	6	4.97	11	5.22	7	5.30
8	United Arab Emirates	20.89	6	7.26	14	2.71	5	6.12	8	4.79
9	New Zealand	20.75	2	7.92	12	3.26	16	4.14	5	5.43
10	South Korea	20.71	14	5.78	9	4.24	4	6.32	11	4.38
11	Japan	20.28	12	5.93	7	4.79	3	6.55	16	3.01
12	Austria	20.00	9	6.73	11	3.69	8	5.66	13	3.91
13	France	19.44	13	5.92	10	4.03	13	4.94	10	4.55
14	Australia	19.40	11	6.01	13	3.18	9	5.43	9	4.78
15	Spain	14.58	15	4.95	16	2.21	14	4.69	17	2.72
16	China	13.94	16	4.38	15	2.25	15	4.18	15	3.13
17	Brazil	7.17	20	0.93	18	0.86	19	1.89	14	3.49
18	Russia	7.09	17	2.58	20	0.52	20	1.64	18	2.35
19	Mexico	6.51	19	1.16	17	1.01	17	2.34	19	2.00
20	India	6.14	18	1.41	19	0.54	18	2.28	20	1.91

Source: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf

Appendix 2

Israel Tech Chart



Source: https://robohub.org/israel-a-land-flowing-with-ai-and-autonomous-cars/

About the Author

Attilio M. Costabel, Esq., is an Adjunct Professor of Law at the St. Thomas University School of Law in Florida.

To Cite this Article

Costabel, A. M. (2018, Fall). The Internet of Things: The future was yesterday. *Journal of Multidisciplinary Research, 10*(3), 7-21.

”Golden Gate Bridge in San Francisco Bay”
2019

Photography by Scott Gillig

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 23-44.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Survey on the Regulations of Autonomous Vehicles

Lindsey Brock
Rumrell, McLeod, & Brock, PLLC

and

Lindsay Tropnas
Rumrell, McLeod, & Brock, PLLC

Abstract

This article covers the regulatory landscape of "autnomous vehicles" in the United States, with notions and history of artificial intelligence applied to autonomous systems. Part 1 deals with General Rules, Federal and State, about guidance, safety and perfotmance standards, operation of autonomous vehicles on public roads and testing of autonomous vehicles. Part 2 covers regulatory issue by States, beginning with California and Nevada (this latter being the first state to authorize the operation of autonomous vehicles in 2011) and 21 other states that followed up: Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Louisiana, Michigan, New York, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, and Vermont—and Washington D.C. The article concludes that there is a clear trend that states are moving toward some level of acceptance of autonomous vehicle technology and that the future and the current liability schemes will either adapt to fit the emerging technologies or new standards should develop through legal precedent or legislative action. The article poses some questions at the end.

Keywords: autonomous vehicles, regulation, safety, standards

Introduction

The world is facing an unprecedented emergence of artificial intelligence and autonomous systems. In the transportation sector, where 9 out of 10 serious roadway crashes occur due to human error, automated vehicle technologies possess the potential to save thousands of lives, as well as reduce congestion, enhance mobility, and improve productivity.[80] Governments around the world are quickly recognizing the data protection implications of smart cars, and reacting.[81] For example, the German Ethics Commission recently reported that user consent is required to use vehicle data for any reason beyond safety.[82] European and North American countries such as the United States, Germany, United Kingdom, and Netherlands were pioneers of self-driving vehicle licensing and have introduced regulations for self-driving cars on public roads and issued autonomous testing permits.[83] Asian countries quickly caught up and have been enacting similar legislation over the last three years.[84] In Canada, automakers have engaged federal privacy officials to understand compliance requirements when developing new smart car technologies that are inevitably accompanied by privacy implications.[85]

Motivated by the unprecedented spike in automotive fatalities in 2015, mostly caused by human error, the United States Department of Transportation (USDOT), through the National Highway Traffic Safety Administration (NHTSA), has embraced self-driving cars as a means to significantly reduce motor vehicle crashes.[86] Safety remains the number one priority for the USDOT and is the specific focus of the NHTSA.[87] Because current legislation and policies have not caught up with technology, the U.S. Congress and the USDOT are hoping to create legislation and regulations that balance technology and car manufacturers' freedom to test, evaluate, and deploy driverless cars the develop best practices to operate and govern these vehicles on U.S. roadways.[88]

[80] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[81] The Virtual Highway – Smart Cars Driven by Smart Data (March 2, 2018), https://www.lexology.com/library/detail.aspx?g=63646f28-c82e-4322-bfc2-78eff36b7a6b

[82] The Virtual Highway – Smart Cars Driven by Smart Data (March 2, 2018), https://www.lexology.com/library/detail.aspx?g=63646f28-c82e-4322-bfc2-78eff36b7a6b

[83] Global Survey of Autonomous Vehicle Regulations (March 15, 2018), https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[84] Global Survey of Autonomous Vehicle Regulations (March 15, 2018), https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[85] The Virtual Highway – Smart Cars Driven by Smart Data (March 2, 2018), https://www.lexology.com/library/detail.aspx?g=63646f28-c82e-4322-bfc2-78eff36b7a6b

[86] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[87] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[88] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

Part I: General Rules: State and Federal

Federal Guidance for Automated Driving Systems

In September 2017, the USDOT and the NHTSA released new federal guidance for *Automated Driving Systems (ADS): A Vision for Safety 2.0.*[89] This is the latest guidance for automated driving systems to industry and States. Since the USDOT was established in 1966, there have been more than 2.2 million motor-vehicle-related fatalities in the United States.[90] In addition, after decades of decline, motor vehicle fatalities spiked by more than 7.2 percent in 2015, the largest single-year increase since 1966.[91] The major factor in 94 percent of all fatal crashes is human error.[92] So, ADSs have the potential to significantly reduce highway fatalities by addressing the root cause of these tragic crashes.[93] The Department released *A Vision for Safety* to promote improvements in safety, mobility, and efficiency through ADSs. *A Vision for Safety* replaces the *Federal Automated Vehicle Policy* released in 2016.[94] This updated policy framework offers a path forward for the safe deployment of automated vehicles by: (1) encouraging new entrants and ideas that deliver safer vehicles; (2) making Department regulatory processes more nimble to help match the pace of private sector innovation; and (3) supporting industry innovation and encouraging open communication with the public and with stakeholders.[95] From reducing crash-related deaths and injuries, to improving access to transportation, to reducing traffic congestion and vehicle emissions, automated vehicles hold significant potential to increase productivity and improve the quality of life for millions of people.[96]

Safety and Performance Standards

Following NHTSA's guidance, Congress has taken steps to adopt safety and performance standards for autonomous vehicles.[97] Both houses of Congress have worked toward establishing

[89] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[90] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[91] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[92] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[93] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[94] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[95] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[96] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[97] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

relevant safety standards.[98] In September 2017, the United States House of Representatives passed House Bill HR 3388 entitled, "Safely Ensuring Lives Future Development and Research in Vehicle Evolution or SELF-DRIVE."[99] This is the first piece of legislation for regulating autonomous vehicles.[100] Presently, the Senate is considering its own similar bipartisan bill, "American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act" or "AV START Act," which the U.S. Senate Committee on Commerce, Science, and Transportation unanimously approved in October 2017.[101] The House and Senate Bills are largely similar, non-partisan, and non-controversial, setting the stage for adoption of a federal regulatory scheme for autonomous vehicles in 2018.[102] Both bills provide NHTSA exclusive control over regulating the design, construction and performance of autonomous vehicles, as is currently the case.[103] The bills include provisions addressing cybersecurity, privacy and consumer education. Regulating these areas in a consistent manner is vital to maintaining the safety and security of the motoring public.[104] As to cybersecurity, autonomous vehicle manufacturers will be required to adopt plans to identify reasonably foreseeable vulnerabilities and the means to mitigate such risks; as, for example, ways to keep malicious commands from remotely taking over self-driving cars.[105] Given the realistic concerns over consumer privacy with today's technology, issues related to the more technologically advanced self-driving cars is of even greater import.[106] Accordingly, the regulations would require implementation of plans to describe the information collected, how the information would be

[98] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[99] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[100] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[101] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[102] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[103] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[104] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[105] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[106] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

used and steps taken to prevent unauthorized disclosure of such information.[107] Public education regarding the capabilities and limitations of autonomous vehicles is also instrumental to an effective regulatory regime.[108] Although the House bill encourages access to autonomous vehicles for the elderly and disabled, the Senate bill specifically prohibits states from discriminating against people with disabilities by enacting laws that would, for example, require a licensed driver to be in the car at all times.[109]

Vehicles Operating on Public Roads

Vehicles operating on public roads are generally subject to both federal and state jurisdiction, and States are beginning to draft legislation to deploy safely emerging ADSs.[110] These practices for aiding in the development and integration of autonomous vehicles maintain the current division of responsibility between the state and federal governments; specifically, the USDOT retains responsibility for regulating motor vehicle safety including setting and enforcing Federal Motor Vehicle Safety Standards (FMVSS).[111] Under the proposed federal regime, state laws contrary to those promulgated by the USDOT are pre-empted.[112] Nevertheless, states continue to have authority over vehicle registration, licensure, insurance, traffic laws and crash investigations.[113] To support the work at the state level, NHTSA offers Section 2: Technical Assistance to States, Best Practices for Legislatures Regarding Automated Driving Systems (Best Practices).[114] The section clarifies and delineates federal and state roles in the regulation of ADSs.[115] NHTSA remains responsible for regulating the safety design and performance aspects of motor vehicles and motor vehicle equipment; states continue to be responsible for regulating the human driver and vehicle operations.[116]

---

[107] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[108] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[109] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[110] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[111] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[112] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[113] The federal landscape on self-driving cars – Lexology (February 15, 2018), https://www.lexology.com/library/detail.aspx?g=65fe4f43-163d-4bfd-b3fe-87ab4370bfbf&filterId=1c51e973-6220-44ec-9899-dca501ffaa0

[114] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[115] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[116] Automated Driving Systems 2.0: A Vision for Safety (September 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

Testing of Autonomous Vehicles

There have been some setbacks in the testing of autonomous vehicles. An Uber vehicle with a safety driver struck and killed a pedestrian in Tempe, Arizona on March 18, 2018; Uber quickly suspended all testing of its autonomous fleet while it investigates the causes of the crash.[117] On March 23, 2018, the driver of a Tesla in autonomous mode died when the vehicle crashed into a highway median in Mountain View, California.[118] Tesla has not suspended the feature in its vehicles while the company and the NHTSA investigate the causes of that crash.[119] Since proponents highlight the safety improvements of driverless cars, these fatalities will invite stricter scrutiny of the claims of the technology.[120] Despite the fatal accidents involving semi-autonomous cars occurring within days of each other in March 2018, testing of the automated vehicle technology continues.[121] As an emerging technology, it is understandable that stricter safety scrutiny will occur for these autonomous systems. Near perfect operation is expected from the public and there is a low tolerance for any errors. Nevertheless, proportionately, the autonomous vehicle systems have a better safety record than human operated vehicles.

Part II: State Actions

California is undoubtedly the top-ranked state in openness and preparedness for autonomous vehicles.[122] Its autonomous vehicle testing regulations were introduced in September 2014 and required a driver be in the vehicle, ready to assume control.[123] On April 2, 2018, California expanded its testing rules to allow for remote monitoring instead of a safety driver inside the vehicle.[124] California's most recent Bill Number AB 1592 (2016) authorizes the Contra Costa Transportation Authority to conduct a pilot project for the testing of autonomous vehicles that are not equipped with a steering wheel, a brake pedal, an accelerator, or an operator inside the vehicle, if the testing is conducted only at specified locations and the autonomous vehicle operates at specified speeds.[125] Bill Number AB 669 (2017) extends the sunset date of the law allowing the testing of vehicle platooning with less than 100 feet between each vehicle

[117] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[118] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[119] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[120] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[121] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[122] Global Survey of Autonomous Vehicle Regulations (March 15, 2018), https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[123] Global Survey of Autonomous Vehicle Regulations (March 15, 2018), https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[124] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[125] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

from January 2018 to January 2020.[126] The bill also prohibits someone from participating in the testing, unless they hold a valid driver's license for the class of vehicle.[127]

Bill Number SB 145 (2017) repeals a requirement that the Department of Motor Vehicles (DMV) notifies the Legislature of receipt of an application seeking approval to operate an autonomous vehicle capable of operating without the presence of a driver inside the vehicle on public roads.[128] It also repeals the requirement that the approval of such an application is not effective any sooner than a specified number of days after the date of the application.[129] Lastly, Bill Number SB 1 (2017) encourages the California DOT and cities and counties to, when possible, cost-effective and feasible, use funds under the Road Maintenance and Rehabilitation Program to use advanced technologies and communications systems in transportation infrastructure that recognize and accommodate advanced automotive technologies that may include, but are not necessarily limited to, charging or fueling opportunities for zero-emission vehicles, and provision of infrastructure-to-vehicle communications for transitional or fully autonomous vehicle systems.[130]

While neighboring states Arizona and Nevada also allow testing without a safety driver, California is both the most populous state and the home to many of the companies' testing vehicles.[131] Each U.S. state is responsible for its own autonomous driving legislation.[132] According to an article from the National Conference of State Legislatures called "Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation," dated May 21, 2018, Nevada was the first state to authorize the operation of autonomous vehicles in 2011.[133] Since then, 21 other states—Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Louisiana, Michigan, New York, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, and Vermont—and Washington D.C. have passed legislation related to autonomous vehicles.[134] Governors in Arizona, Delaware, Hawaii, Idaho, Maine,

[126] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[127] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[128] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[129] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[130] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[131] The state of self-driving car laws across the U.S. (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/

[132] Global Survey of Autonomous Vehicle Regulations (March 15, 2018), https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[133] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[134] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Massachusetts, Minnesota, Ohio, Washington, and Wisconsin have issued executive orders related to autonomous vehicles.[135] Currently, there remain about 19 states and territories that have not enacted legislation, or executive orders, or both, regarding autonomous vehicles: Alaska, American Samoa, Guam, Iowa, Kansas, Maryland, Missouri, Montana, New Hampshire, New Jersey, New Mexico, Northern Mariana Islands, Oklahoma, Puerto Rico, Rhode Island, South Dakota, Virgin Islands, West Virginia, and Wyoming.[136] Below you will find the different bills and executive orders that several different states have passed or issued recently, in addition to the above California legislation and regulations.

Alabama. Pursuant to Bill Number SB 125 (2018), Alabama seeks to regulate the partially autonomous systems involved in truck platooning. The bill defined a truck platoon as "a group of individual commercial trucks traveling in a unified manner at electronically coordinated speeds at following distances that are closer than would be reasonable and prudent without the electronic coordination."[137] A human operator is still present within the vehicles. The bill also exempts the trailing trucks in a truck platoon from the state's following too closely provisions if the truck platoon is engaged in electronic brake coordination and any other requirement imposed by the DOT by rule.[138]

Arkansas passed a bill regulating the testing of vehicles with autonomous technology, and related to vehicles equipped with driver-assistive truck platooning systems under Bill Number HB 1754 (2017).[139]

Arizona's Governor Doug Ducey signed an executive order in late August 2015 directing various agencies to "undertake any necessary steps to support the testing and operation of self-driving vehicles on public roads within Arizona."[140] He also ordered the enabling of pilot programs at selected universities and developed rules to be followed by the programs.[141] The order established a Self-Driving Vehicle Oversight Committee within the governor's office.[142] In

[135] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[136] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[137] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[138] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[139] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[140] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[141] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[142] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

March 2018, Governor Ducey added to the 2015 executive order with Executive Order 2018-04.[143] The order includes updates to keep pace with emerging technology, including advancements toward fully autonomous vehicles, as well as requiring all automated driving systems to be in compliance with all federal and state safety standards.[144]

Colorado recently passed Bill Number SB 213 (2017), which allows a person to use an automated driving system to drive or control a function of a motor vehicle, if the system is capable of complying with every state and federal law that applies to the function that the system is operating.[145] The bill requires approval for vehicle testing if the vehicle cannot comply with every relevant state and federal law.[146] Finally, the bill requires the Colorado DOT to submit a report on the testing of automated driving systems.[147]

Connecticut recently passed Bill Number SB 260 (2017), which requires the development of a pilot program for up to four municipalities for the testing of fully autonomous vehicles on public roads in those municipalities.[148] The bill specifies the requirements for testing, including having an operator seated in the driver's seat and providing proof of insurance of at least $5 million.[149] The bill establishes a task force to study fully autonomous vehicles; and the study must include an evaluation of NHTSA's standards regarding state responsibility for regulating Autonomous Vehicles (AV), an evaluation of laws, legislation and regulations in other states, recommendations on how Connecticut should legislate and regulate AVs, and an evaluation of the pilot program.[150] **Delaware's** Governor John Carney signed an executive order in September 2017 establishing the Advisory Council on Connected and Autonomous Vehicles, tasked with developing recommendations for innovative tools and strategies that can be used to prepare Delaware's transportation network for connected and autonomous vehicles.[151]

---

[143] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[144] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[145] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[146] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[147] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[148] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[149] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[150] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[151] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Florida's 2016 legislation expanded the operation of autonomous vehicles on public roads and eliminated requirements related to the testing of autonomous vehicles and the presence of a driver in the vehicle.[152] Florida passed Bill Number HB 1207 (2012), which declared a legislative intent to encourage the safe development, testing and operation of motor vehicles with autonomous technology on public roads of the state and finds that the state does not prohibit or specifically regulate the testing or operation of autonomous technology in motor vehicles on public roads.[153] Moreover, it authorizes a person who possesses a valid driver's license to operate an autonomous vehicle, specifying that the person who causes the vehicle's autonomous technology to engage is the operator.[154] It also authorizes the operation of autonomous vehicles by certain persons for testing purposes under certain conditions and requires insurance, a surety bond or self-insurance prior to the testing of a vehicle.[155] Finally, it directs the Florida Department of Highway Safety and Motor Vehicles to prepare a report recommending additional legislative or regulatory action that may be required for the safe testing and operation of vehicles equipped with autonomous technology, to be submitted no later than February 12, 2014.[156] Florida passed Bill Number HB 7027 (2016), which permits operation of autonomous vehicles on public roads by individuals with a valid driver license.[157] This bill eliminates the requirement that a driver is present in the vehicle.[158] Similar to Alabama, Florida has also allowed for testing of truck platooning on limited highways in the state.

Georgia recently passed Bill Number HB 472 (2017), which specifies that the law prohibiting following too closely does not apply to the non-leading vehicle in a coordinated platoon.[159] The bill also defines coordinated platoon as a group of motor vehicles traveling in the same lane utilizing vehicle-to-vehicle communication technology to automatically coordinate the

[152] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[153] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[154] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[155] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[156] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[157] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[158] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[159] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

movement of the vehicles.[160] Georgia also passed Bill Number SB 219 (2017), which exempts a person operating an automated motor vehicle with the automated driving system engaged from the requirement to hold a driver's license.[161] The bill also specifies conditions that must be met for a vehicle to operate without a human driver present in the vehicle, including insurance and registration requirements.[162]

Hawaii's Governor David Ige signed an executive order in November 2017 establishing a connected autonomous vehicles (CAV) contact in the governor's office and requires certain government agencies to work with companies to allow for self-driving vehicle testing in the state.[163]

Idaho's Governor C.L. "Butch" Otter signed Executive Order 2018-01 on January 2, 2018 to create the Autonomous and Connected Vehicle Testing and Deployment Committee to identify relevant state agencies to support the testing and deployment of autonomous and connected vehicles, discuss how best to administer the testing of autonomous and connected vehicles in relation to issues such as vehicle registration, licensing, insurance, traffic regulations, and vehicle owner or operator responsibilities and liabilities under current law, review existing state statutes and administrative rules and identify existing laws or rules that impede the testing and deployment of autonomous and connected vehicles on roads and identify strategic partnerships to leverage the social, economic, and environmental benefits of autonomous and connected vehicles.[164] The committee must include two members of the Idaho Legislature, one appointed by the Speaker of the House and one appointed by the President Pro Tempore of the Senate.[165]

Illinois recently passed Bill Number HB 791 (2017), which preempts local authorities from enacting or enforcing ordinances that prohibit the use of vehicles equipped with Automated Driving Systems.[166] The bill also defines "automated driving system-equipped vehicle."[167]

---

[160] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[161] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[162] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[163] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[164] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[165] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[166] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[167] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Indiana recently passed Bill Number HB 1290 (2018), which defines "Vehicle platoon" to mean a group of motor vehicles that are traveling in a unified manner under electronic coordination at speeds and following distances that are faster and closer than would be reasonable and prudent without electronic coordination.[168] The bill clarifies vehicle platooning is exempt from the following too close provisions of three hundred feet.[169] The bill also lays out an approval system for vehicle platooning in the state, including requiring the person or organization to file a plan for general vehicle platoon operations with the transportation commissioner.[170]

Kentucky recently passed Bill Number SB 116 (2018), which allows a motor carrier to operate a platoon on Kentucky's highways if the motor carrier provides notification to the Kentucky Department of Vehicle Regulation (DVR) and the Kentucky State Police, including a plan for general platoon operations.[171] The DVR then has thirty days from the date of receipt to review the notification plan submitted and approve or reject the plan.[172] If the department rejects a submitted plan, it must inform the motor carrier of the reason for the rejection and provide guidance on how to resubmit the notification and plan to meet the standards.[173] Only commercial motor vehicles shall be eligible to operate in a platoon.[174] An appropriately endorsed driver who holds a valid commercial driver's license shall be present behind the wheel of each commercial motor vehicle in a platoon.[175] A commercial motor vehicle involved in a platoon shall not draw another motor vehicle in the platoon.[176] Each commercial motor vehicle involved in a platoon shall display a marking warning other motorists and law enforcement that the vehicle may be

[168] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[169] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[170] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[171] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[172] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[173] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[174] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[175] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[176] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

part of a platoon.[177] The department shall promulgate administrative regulations to set forth procedures for platooning, including required elements of a platooning plan.[178] Many of the platooning laws are considered as a first step toward ultimately permitting fully autonomous vehicle operation. The platooning requirement of a human operator in the vehicles provides a certain level of comfort to the general public.

Louisiana passed Bill Number HB 1143 (2016), which defines "autonomous technology" for purposes of Louisiana's Highway Regulatory Act.[179] **Maine's** Governor Paul LePage signed Executive Order 2018-001 on January 17, 2018, creating the Maine Highly Automated Vehicles (HAV) Advisory Committee to oversee the beneficial introduction to Maine of Highly Automated Vehicle technologies, and assessing, developing and implementing recommendations regarding potential Pilot Projects initiated to advance these technologies.[180] The committee is directed to evaluate and make recommendations regarding proposed HAV Pilot Projects and require interested parties to contact the committee and apply for a permit prior to operating pilot vehicles on public roadways in Maine.[181] Maine also recently passed Bill Number HP 1204 (2018), which created the Commission on Autonomous Vehicles to coordinate efforts among state agencies and knowledgeable stakeholders to inform the development of a process to allow an autonomous vehicle tester to demonstrate and deploy for testing purposes an automated driving system on a public way.[182] The commission will consist of at least 11 members.[183] By January 15, 2020, Maine's Commissioner of Transportation is to submit an initial written report on the progress of the commission and by January 15, 2022, the Commissioner will submit a final written report that includes findings and recommendations, including suggested legislation, for presentation to the joint standing committee of the Maine Legislature having jurisdiction over transportation matters.[184]

[177] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[178] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[179] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[180] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[181] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[182] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[183] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[184] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Massachusetts' Governor Charlie Baker signed an executive order in October 2016, "To Promote the Testing and Deployment of Highly Automated Driving Technologies."[185] The order created a working group on AVs and the group is expected to work with experts on vehicle safety and automation, work with members of the legislature on proposed legislation, and support agreements that AV companies will enter with the state DOT, municipalities and state agencies.[186] **Michigan** passed Bill Number SB 995 (2016), which allows for autonomous vehicles under certain conditions. The legislation allows operation without a person in the autonomous vehicle.[187] The bill also specifies that the requirement that commercial vehicles maintain a minimum following distance of 500 feet does not apply to vehicles in a platoon.[188] Bill Number SB 996 (2016) allows for autonomous vehicles under certain conditions.[189] The legislation also allows operation without a person in the autonomous vehicle.[190] Bill Number SB 998 (2016) exempts mechanics and repair shops from liability on fixing automated vehicles.[191]

Minnesota's Governor Mark Dayton issued Executive Order 18-04 on March 5, 2018, establishing a Governor's Advisory Council on Connected and Automated Vehicles to study, assess, and prepare for the transformation and opportunities associated with the widespread adoption of automated and connected vehicles.[192] Perhaps to depoliticize or to insure bipartisanship, the advisory council must include one member from each party from each legislative chamber.[193]

Mississippi recently passed Bill Number HB 1343 (2018), which defines "Platoon" to mean a group of individual motor vehicles traveling in a unified manner at electronically coordinated speeds at following distances that are closer than would be reasonable and prudent

[185] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[186] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[187] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[188] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[189] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[190] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[191] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[192] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[193] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

without such coordination.[194] The bill also creates an exemption from the state's following too closely traffic law for the operator of a nonlead vehicle in a platoon, if the platoon is operating on a limited access divided highway with more than one lane in each direction and the platoon consists of no more than two motor vehicles.[195] A platoon may be operated in Mississippi only after an operator files a plan for approval of general platoon operations with the state's Department of Transportation.[196] If that department approves the submission, it shall forward the plan to the Department of Public Safety for approval.[197] The plan shall be reviewed and either approved or disapproved by the Department of Transportation and the Department of Public Safety within thirty days after it is filed.[198] If approved by both departments, the operator shall be allowed to operate the platoon five working days after plan approval.[199] The Motor Carrier Division of the Department of Public Safety is directed to develop the acceptable standards required for each portion of the plan.[200]

Nebraska recently passed Bill Number LB 989 (2018), which states that a driverless-capable vehicle may operate on public roads in the state without a conventional human driver physically present in the vehicle, as long as the vehicle meets the following conditions: (1) The vehicle is capable of achieving a minimal risk condition if a malfunction of the automated driving system occurs that renders the system unable to perform the entire dynamic driving task within its intended operational design domain, if any; and (2) While in driverless operation, the vehicle is capable of operating in compliance with the applicable traffic and motor vehicle safety laws and regulations of this state that govern the performance of the dynamic driving task, including, but not limited to, safely negotiating railroad crossings, unless an exemption has been granted by the DMV.[201] The bill also clarifies responsibilities in the event of a crash or collision: (1) The automated-driving-system-equipped vehicle shall remain on the scene of the crash or collision and the owner of the automated-driving-system-equipped vehicle, if capable, or a

[194] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[195] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[196] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[197] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[198] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[199] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[200] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[201] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

person on behalf of the automated-driving-system-equipped vehicle owner, shall report any crash or collision.[202] The DMV is the sole and exclusive state agency that may implement this act.[203]

Nevada recently passed Bill Number AB 69 (2017), which defines terms including "driver-assistive platooning technology," "fully autonomous vehicle" and "automated driving system."[204] The bill allows the use of driver-assistive platooning technology on highways in the state.[205] The bill also requires the reporting of any crashes to the department of motor vehicles within 10 days if the crash results in personal injury or property damage greater than $750.[206] The bill allows a fine of up to $2,500 to be imposed for violations of laws and regulations relating to autonomous vehicles.[207] The bill permits the operation of fully autonomous vehicles in the state without a human operator in the vehicle.[208] Finally, the bill specifies that the original manufacturer is not liable for damages if a vehicle has been modified by an unauthorized third party.[209] **New York** recently passed Bill Number AB 9508 (2018), which discusses autonomous vehicle demonstrations and tests and states that such tests and demonstrations shall only take place under the direct supervision of the New York state police and in a form and manner prescribed by the superintendent of the New York state police.[210] Additionally, a law enforcement interaction plan shall be included as part of the demonstration and test application that includes information for law enforcement and first responders regarding how to interact with such a vehicle in emergency and traffic enforcement situations.[211]

[202] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[203] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[204] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[205] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[206] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[207] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[208] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[209] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[210] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[211] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

North Carolina recently passed Bill Number HB 469 (2017), which establishes for the operation of fully autonomous motor vehicles on public highways of that state.[212] The bill specifies that a driver's license is not required for an AV operation, and it requires an adult be in the vehicle if a person under 12 is in the vehicle.[213]

North Dakota recently passed Bill Number 1202 (2017), which requires the DOT to study the use of vehicles equipped with automated driving systems on the highways in this state and the data or information stored or gathered using those vehicles.[214] The bill also requires that the study include a review of current laws dealing with licensing, registration, insurance, data ownership and use, and inspection and how they should apply to vehicles equipped with automated driving systems.[215]

Ohio's Governor John Kasich signed Executive Order 2018-01K on January 18, 2018.[216] The order created "DriveOhio" to, in part, "bring together those who are responsible for building infrastructure in Ohio with those who are developing the advanced mobility technologies needed to allow our transportation system to reach its full potential by reducing serious and fatal crashes and improving traffic flow."[217] Ohio Governor Kasich signed Executive Order 2018-O4K in May of 2018, allowing autonomous vehicles testing and pilot programs in the state.[218] In order to do so, companies must register with DriveOhio (created by the January 2018 EO) and submit information on their companies, intended areas and conditions to test in and other requirements.[219] Autonomous vehicles tested in the state must have a designated operator, although they are not required to be inside the vehicle.[220]

Oregon recently passed Bill Number HB 4063 (2018), which establishes a Task Force on Autonomous Vehicles and clarifies that the state Department of Transportation is the lead agency

[212] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[213] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[214] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[215] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[216] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[217] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[218] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[219] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[220] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

responsible for coordination of autonomous vehicle programs and policies.[221] The Task Force will consist of 31 members, including two members from the Senate and two members from the House, with each chamber represented by one member of each party.[222] Members of the legislature appointed to the task force are nonvoting members and may act in an advisory capacity only.[223] The task force shall develop recommendations for legislation to be introduced during the next odd-numbered year regular session of the Legislative Assembly regarding the deployment of autonomous vehicles on highways.[224] The proposed legislation shall be consistent with federal law and guidelines and shall address the following issues: (A) Licensing and registration; (B) Law enforcement and accident reporting; (C) Cybersecurity; and (D) Insurance and liability.[225]

Pennsylvania passed Bill Number SB 1267 (2016), which allows the use of allocated funds, up to $40,000,000, for intelligent transportation system applications, such as autonomous and connected vehicle-related technology, in addition to other specified uses.[226] **South Carolina** recently passed Bill Number HB 3289 (2017), which specifies that minimum following distance laws for vehicles traveling along a highway does not apply to the operator of any non-leading vehicle traveling in a platoon.[227]

Tennessee recently passed SB 151 (2017), which created the "Automated Vehicles Act."[228] The bill modifies laws related to unattended motor vehicles, child passenger restraint systems, seat belts, and crash reporting in order to address ADS-operated vehicles.[229] The bill

[221] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[222] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[223] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[224] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[225] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[226] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[227] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[228] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[229] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

specifies that ADS-operated vehicles are exempt from licensing requirements.[230] The bill permits ADS-operated vehicles on streets and highways in the state without a driver in the vehicle if it meets certain conditions.[231] The bill specifies that the ADS shall be considered a driver for liability purposes when it is fully engaged and operated properly.[232] The bill makes it a class A misdemeanor to operate a motor vehicle on public roads in the states without a human driver in the driver's seat without meeting the requirements of the Automated Vehicles Act.[233] Finally, the bill specifies that the Automated Vehicles Act only applies to vehicles in high or full automation mode.[234]

Texas recently passed Bill Number 1791 (2017), which allows the use of a connected braking system in order to maintain the appropriate distance between vehicles.[235] The bill specifies that "connected braking system" means a system by which the braking of one vehicle is electronically coordinated with the braking system of following a vehicle.[236] Bill Number SB 2205 (2017) specifies that the owner of an automated driving system is the operator of the vehicle when the system is engaged and the system is considered licensed to operate the vehicle.[237] Allows an automated motor vehicle to operate in the state regardless of whether a human operator is present in the vehicle, as long as certain requirements are met.[238] **Utah** recently passed Bill Number SB 56 (2018), which defines a "connected platooning system" to mean a system that uses vehicle-to-vehicle communication to electronically coordinate the speed and braking of a lead vehicle with the speed and braking of one or more following vehicles.[239]

[230] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[231] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[232] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[233] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[234] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[235] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[236] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[237] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[238] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[239] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Virginia passed Bill Number HB 454 (2016), which allows the viewing of a visual display while a vehicle is being operated autonomously.[240]

Vermont recently passed Bill Number HB 494 (2017), which requires the DOT to convene a meeting of stakeholders with expertise on a range of topics related to automated vehicles.[241] The secretary of transportation must report to the House and Senate committees on transportation regarding the meetings and any recommendations related automated vehicles, including proposed legislation.[242]

Washington's Governor Jay Inslee signed an executive order in June 2017 to address autonomous vehicle testing and establish an autonomous vehicle workgroup.[243] The order requires that state agencies with pertinent regulator jurisdiction "support the safe testing and operation of autonomous vehicles on Washington's public roads."[244] It establishes an interagency workgroup and enables pilot programs throughout the state.[245] The order specifies certain requirements for vehicles operated with human operators present in the vehicle and for vehicles operated without human operators in the vehicle.[246]

Washington, D.C. passed Bill Number 2012 DC B 19-0931, which defines "autonomous vehicle" as "a vehicle capable of navigating District roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle's control systems."[247] The bill requires a human driver "prepared to take control of the autonomous vehicle at any moment."[248]

[240] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[241] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[242] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[243] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[244] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[245] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[246] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[247] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[248] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

The bill restricts conversion to recent vehicles, and addresses the liability of the original manufacturer of a converted vehicle.[249]

Wisconsin's Governor Scott Walker signed an executive order in May 2017 creating the Governor's Steering Committee on Autonomous and Connected Vehicle Testing and Deployment.[250] The committee is tasked with advising the governor "on how best to advance the testing and operation of autonomous and connected vehicles in the State of Wisconsin."[251] The order specifies the members of the committee, including six legislators from the state.[252] The duties of the committee include identifying all agencies in the state with jurisdiction over testing and deployment of the vehicles, coordinating with the agencies to address concerns related to issues such as "vehicle registration, licensing, insurance, traffic regulations, equipment standards, and vehicle owner or operator responsibilities and liabilities under current law," and reviewing current state laws and regulations that may impede testing and deployment, along with other tasks.[253] The state department of transportation is required to submit a final report to the governor by June 30, 2018.[254] Wisconsin also recently passed Bill Number SB 695 (2018), which defines a "platoon" as a group of individual motor vehicles traveling in a unified manner at electronically coordinated speeds.[255] This bill creates an exception for platoons to the traffic law requiring the operator of a motor truck with a gross weight of more than 10,000 pounds to maintain a distance of not less than 500 feet behind the vehicle immediately preceding.[256]

[249] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[250] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[251] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[252] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[253] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[254] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[255] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[256] Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (May 21, 2018), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

Conclusion

Based on the different legislation and executive orders that have been passed or issued in the various states, there is a clear trend that states are moving toward some level of acceptance of autonomous vehicle technology. Even in the states that are currently allowing only platooning as a first step, it is still a first step toward the acceptance of these new technologies.

Many states are creating conditions where an autonomous vehicle may be permitted to operate without an operator having a driver's license or there even being a person in the vehicle during its operation. This is very important because as discussed above, for example, the US Senate's bill specifically prohibits states from discriminating against people with disabilities by enacting laws that would, for example, require a licensed driver to be in the car at all times.

Those states that require a licensed driver to be in the vehicle with an individual that is disabled or that limit a disabled driver's rights in operating an autonomous vehicle may encounter future legal challenges over the preemption of these requirements by the federal laws and regulations.

Certain states have taken preemptive action to reduce third party liability related to the repair and operation of these autonomous systems. In relation to product liability schemes within the common law, it will be interesting to follow the development of any litigation over errors in the autonomous systems that result in traffic crashes; in particular, as new improvements are developed into the operating systems.

All these will be questions for the future, as the current liability schemes either adapt to fit these emerging technologies, or new standards are developed through legal precedent or legislative action.

About the Authors

Lindsay Brock, Esq., is an attorney with Rumrell, McLeod, & Brock, PLLC.

Lindsay Tropnas, Esq., is an attorney with Rumrell, McLeod, & Brock, PLLC.

Discussion Questions

1. One can envision where vehicles with older, potentially less safe operating systems, are involved in a crash. The question then arises whether it was negligent for the vehicle owner to operate the vehicle without installing the available software update to the autonomous system.

2. What if there is a cost for the update?

3. Are the software updates considered recalls?

To Cite this Article

Brock, L., & Tropnas, L. (2018, Fall). Survey on the regulations of autonomous vehicles. *Journal of Multidisciplinary Research, 10*(3), 23-44.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 45-60.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Disruptive Technologies and Business Models: Emerging Regulatory Issues from the Sharing Economy

Andrew M. Danas
Grove, Jaskiewicz, and Cobert LLP [257]

The technological revolution that many are calling the new or Fourth Industrial Revolution[258] is manifesting itself in multiple ways, with the development of "smart" phones, autonomous vehicles, ships, drones, robots, and devices and products connected through the Internet. The development of such devices has led to new business models, disrupting both existing industries and their related rules and regulations. If predictions are correct, we are just at the starting point of a vast new set of businesses based on Platform Services and the "Internet of Things" (IoT).

In addition to introducing new ways of doing business, these new products and services bring with them corresponding questions of regulation and liability. Specifically, who is providing the service and what services are being provided? Who bears responsibility when things go wrong or when new technology is used for unlawful purposes? Can the responsible parties satisfy their obligations to pay damages in the event of liability? Can the market and industry self-regulate the relationship between providers and consumers, or should the government establish consumer protection rules? If rules are required, should existing rules be used or is a new regulatory template required?

These issues will exist when autonomous vehicles drive on roads; when elevator manufacturers remotely manage their daily operations; and when ships are no longer manned but are instead operated by remote control. How the courts and legislatures address these issues will be crucial to the successful transition to a connected society based on IoT and digitalized products and services.

The recent market disruptions created by businesses providing services based on Peer to Peer networks, commonly called the "Sharing Economy" or "Platform Services," provide an early road map of the types of regulatory, liability, and insurance issues that will need to be

[257]. Grove, Jaskiewicz and Cobert, LLP, 1101 17th Street, N.W., Suite 609, Washington, D.C. 20036; 202.296.2900, ext.219; http://www.gjcobert.com; adanas@gjcobert.com

[258]. *See, e.g.,* World Economic Forum, *Fourth Industrial Revolution*; https://toplink.weforum.org/knowledge/insight/a1Gb0000001RIhBEAW/explore/summary

addressed when the coming technologically-based disruptive business models challenge an existing market.

Sharing economy Platforms or Peer-to-Peer Networks ("P2P") are business models based on a computer platform (often in the cloud) that utilize their connections with other computer-connected devices (smart phones included) to facilitate transactions or services between individual buyers and sellers. They rely upon the collection and use of data to facilitate the performance of a service between the two other parties to the transaction.

The two-best known "Sharing Economy" businesses are probably Airbnb and Uber. However, they are not alone. By some estimates over 10,000 new platform companies have been established over the past decade. [259]

This article identifies some of the approaches that have been taken to identify the regulatory issues that have been raised by the development of Platform Services in recent years. It is not a comprehensive survey. Instead, this article is intended to provide an overview of how policy makers have started to grapple with the question of whether and how to regulate these new business models. It primarily focuses on issues related to Uber and ride-sharing companies, simply because that company has been at the forefront of many of the regulatory debates.[260]

As with products based on the Internet of Things ("IoT"), Platform Services rely upon the collection and use of data through an Internet connection to facilitate the provision of the underlying service. In addition, some disruptive Platform Services, such as ride-sharing, may be a transitional stage representing an intermediate step between a new, sharing economy business such as ride sharing to a completely new business, for example, computer-booked rides utilizing automated vehicles. In this context, Platforms share some similarities with IoT products and services and point to some of the same regulatory and legal issues that will be confronted as IoT products and business services become commercially more widespread in the coming years.

This Time It's Different

Technological changes – as with generational changes – are frequently confronted with arguments that what applied in the past should no longer apply in the future because "this time it's different." For example, in the course of human history no society has ever dealt with the introduction of businesses based on new systems of transportation or new forms of

[259]. In her article, *The Law of The Platform*, 101 Minn. L. Rev. 87 (2016), Professor Orly Lobel of the University of San Diego School of Law identified industries affected by the platform economy as including "hotels (Airbnb; Couchsurfing; Homeaway; VRBO); office space (Liquid Space; ShareDesk), parking spaces (ParkingPanda; Park Circa); transportation (Lyft; Sidecar; Uber); restaurants (EatWith; Feastly; Blue Apron; Munchery); used clothing (ThredUp); household tools (Open Shed); outdoor gear (Gearcommons); capital (Zopa; Prosper; Kickstarter; Bitcoin; Kiva); broadcasting (Aereo; FilmOn.com); legal services (Upcounsel); medical services (Healthtap; Teledoc; CrowdMed); academic services (Uguru); everyday errands, such as grocery shopping and laundry (TaskRabbit; Instacart; Airtasker; Washio); and specialized errands, such as flower delivery (BloomThat), dog walking (DogVacay), and package delivery (Shyp)." *Id.* at 95.

[260]. The term "Platform Services" is used in this Article in lieu of the terms the "Sharing Economy" or "Peer-to-Peer Networks." The terms "Sharing Economy" and "Peer-to-Peer Networks" contemplates a situation where there several participants in a transaction that is facilitated by an intermediation software application (the "Platform"). However, as will be discussed, how one defines the service and who is providing it are key to the determination as to how the and what service should be regulated. The term "Platform Services" is used in this Article because it is the introduction and presence of the Platform that is disrupting both the business and the questions involving regulation.

communication. Of course, this is simply not true. Whether it be the introduction of railroads, the telegram, and the telephone; automobiles and radios; or jet planes and facsimile machines, new technologies and business models have consistently created a need to re-examine existing regulatory systems. In other words, we have been here before.

Many of the legal and liability issues faced by regulators in considering the new products and services in the digital age are ultimately definitional. That is, can existing regulatory systems accommodate these new businesses and products, or is a new model needed?

At the core of the regulatory, liability, and insurance issues facing the Fourth Industrial Revolution are thus three different definitional questions. First, is the service or product being provided a traditional service that can or should be subject to existing rules and regulations governing consumer protection, liability, and insurance requirements? Second, how does one define the relationship between the various parties providing the services or products underlying the transaction? Third, what aspects of the services being provided need to be regulated, either to determine liability if things go wrong or to protect against consumer and/or public harm? In other words, are prior reasons for regulation still valid and, if so, will the goal of the regulations still be accomplished or do the new technologies and business methods demand different solutions?

The various – and emerging – regulatory approaches to legal issues involving Platform services hint at possible answers to these questions.

Defining the Service

As a general proposition, there are three ways to categorize services provided by Platforms. First, the Platform and the services it provides are nothing more than a traditional existing service. A taxi is just a taxi. Second, the Platform Service is just a consumer app and software that facilitates services provided by other parties. It is an intermediation tool but it is not the service. Software is just software. Third, the Platform Service is a new hybrid involving both a computer app and a service. Software facilitating individualized services equals something new.

Whether a Platform Service is perceived as being a variation of an existing service or the introduction of a new service frequently turns on the definition of the service being provided. For example, the renting of rooms to travelers has existed and been regulated for centuries. The fact that a computer application facilitates the individual rental of rooms does not mean that the service being provided is not just a rental of rooms or the operation of a hotel. After all, before the computer such rooms could be found by a telephone and before the telephone by telegraph and by letters.

The same analysis also applies to ride-sharing services such as Uber. Livery carriage has existed for centuries. The use of private taxis, and their corresponding regulation, became widespread with the advent of the automobile. The fact that a computer platform is being used to coordinate the ability of riders and drivers to conduct business does not necessarily mean that the basic service is not simply a taxi service.

By way of contrast, Platforms often argue that the only service that they provide is the provision of a computer application that is used by individual consumers and service providers to directly contract with one another for the performance of the underlying transaction. In the case of Uber, this is an individual driver using his or her own automobile to provide transportation

services on an independent contractor basis. The Platforms thus argue that the services provided by the platform are not traditional services and should not be regulated as such.

Courts and government regulators that perceive and define companies such as Uber and Airbnb as providing nothing more than traditional taxi and hotel rental services have generally required them to comply with existing regulations for the comparable industry. The most important example of this approach is a 2017 ruling by the European Court of Justice allowing the regulation of Uber as a transport company.[261] In that case, the ECJ held that that Uber and similar intermediation services are not simply technology companies offering software applications for use as a platform to provide a method for individual passengers to find rides with "non-professional drivers using their own vehicle[s]." Such a service arguably could have been classified as "'an information society service'" subject to the EU's Directives on electronic commerce and a lesser level of regulation.[262] Instead, the ECJ declared that Uber's services are subject to classification as "'a service in the field of transport'" within the meaning of EU law and thus subject to regulation.[263]

In rendering its decision, the European Court of Justice found that the service and software provided by Uber are more than just an intermediary computer program. Instead, they were "indispensable for both the drivers and the persons who wish to make an urban journey."[264] The Court also noted that "Uber exercises decisive influence over the conditions under which the drivers provide their service." [265] Thus, the definition of what was being provided, not just how it was being provided, proved crucial for determining the regulatory status of the digital Platform service.

Another example of a regulatory ruling rejecting the argument that Uber's platform services were just a computer application is a 2016 ruling by the United Kingdom Employment Tribunal. [266] In its ruling, the Tribunal found that Uber is essentially a taxi company and Uber drivers are workers for purposes of the applicable law. Its analysis underlines the crucial role of how the definitional determination of the service being provided affects the determination of whether a Platform Service is providing a new or different type of business service that is or should be subject to existing regulation.

The issue in the UK Employment Tribunal case was the classification of the driver providing services pursuant to the Uber platform and whether the driver was a "worker" under the applicable regulations. As stated by the Tribunal:

---

261. *Asociacion Profesional Elite Taxi v Uber Systems Spain S.L.* ECLI:EU:C:2017:981. A copy of the decision is available at *http://curia.europa.eu/juris/document/document.jsf?text=&docid=198047&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=308369* and at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0434*. *Also see,* Press Release No 136/17, Court of Justice of the European Union, *The Service Provided by Uber Connecting Individuals with Non-Professional Drivers is Covered by Services in the Field of Trans*port (Dec. 20, 2017), *https://curia.europa.eu/jcms/jcms/Jo2_16799* [hereinafter ECJ Press Release].

262. *Id.*

263. *Id.*

264. *Id.*

265. *Id.*

266. Reasons for the Reserved Judgment on Preliminary Hearing Sent to the Parties on 28 October 2016 at ¶ 89, *Aslam, et al v. Uber B.V., et al, Nos. 2202550/2015 & Others,* (U.K.).

86 . . . We have reached the conclusion that any driver who (a) has the App switched on, (b) is within the territory in which he is authorised to work, and (c) is able and willing to accept assignments, is, for so long as those conditions are satisfied, working for Uber under a 'worker' contract and a contract within each of the extended definitions. Our reasons merge and/or overlap in places, but we will endeavour to keep the main strands separate.

87 In the first place, we have been struck by the remarkable lengths to which Uber has gone in order to compel agreement with its (perhaps we should say its lawyers') description of itself and with its analysis of the legal relationships between the two companies, the drivers and the passengers. Any organisation (a) running an enterprise at the heart of which is the function of carrying people in motor cars from where they are to where they want to be and (b) operating in part through a company discharging the regulated responsibilities of a PHV operator, but (c) requiring drivers and passengers to agree, as a matter of contract, that it does not provide transportation services (through UBV or ULL), and (d) resorting in its documentation to fictions, twisted language and even brand new terminology, merits, we think, a degree of scepticism.

Reflecting on the Respondents' general case, and on the grimly loyal evidence of Ms Bertram in particular, we cannot help being reminded of Queen Gertrude's most celebrated line:

The lady doth protest too much, methinks.

88 Second, our scepticism is not diminished when we are reminded of the many things said and written in the name of Uber in unguarded moments, which reinforce the Claimants' simple case that the organisation runs a transportation business and employs the drivers to that end. We have given some examples in our primary findings above. We are not at all persuaded by Ms Bertram's ambitious attempts to dismiss these as mere sloppiness of language.

89 Third, it is, in our opinion, unreal to deny that Uber is in business as a supplier of transportation services. Simple common sense argues to the contrary. The observations under our first point above are repeated. Moreover, the Respondents' case here is, we think, incompatible with the agreed fact that Uber markets a 'product range.'41 One might ask: Whose product range is it if not Uber's? The 'products' speak for themselves: they are a variety of driving services. Mr Aslam does not offer such a range. Nor does Mr Farrar, or any other solo driver. The marketing self-evidently is not done for the benefit of any individual driver. Equally self-evidently, it is done to promote Uber's name and 'sell' its transportation services. In recent proceedings under the title of Douglas O'Connor-v-Uber Technologies Inc. the North California District Court resoundingly rejected the company's assertion that it was a technology company and not in the business of providing transportation services. The judgment included this:

> Uber does not simply sell software; it sells rides. Uber is no more a "technology company" than Yellow Cab is a "technology company" because it uses CB radios to dispatch taxi cabs.

We respectfully agree.[267]

Not every regulator or fact-finder looks at a Platform Services company only to find a traditional business, even if they do not accept the argument that the Platform Services company is only selling a computer application. Ride-sharing companies such as Uber would not have succeeded in claiming they are a new type of business if they had been unable to persuade at least some regulators that they are different from traditional taxi services, even if most regulators find that they are providing more than just a software intermediation platform.

Thus, the third definitional approach to identifying the nature of a Platform Service is to find that the platform is a hybrid of a traditional regulated service and a computer software application. Again, ride sharing companies have led the way with this approach by seeking to identify themselves as Transportation Network Companies (TNCs) and convincing regulators to adopt model legislation recognizing and regulating their services. [268] When adopted at the State level these regulations can have a pre-emptive effect on local jurisdictions that otherwise seek to regulate ride sharing under traditional regulatory standards. [269] The net result of defining a service based on a new technology is to also define a different level of regulation for the service, frequently from local to regional. [270]

The fact that a Platform Service is defined and recognized as a regulatory hybrid has not stopped traditional businesses from challenging either their services or their different form of regulation. Although regulation is frequently tied to consumer protection, it is not the only reason

---

[267]. *Id. at* ¶¶ 86-89 (citing *Douglas O'Connor v. Uber Tech.,* Inc., 82 F. Supp. 3d 1133, 1141 (N.D. Cal. 2015) (other footnotes and citations omitted).

[268]. Although various definitions exist, a Transportation Network Company (TNC) is an organization that uses "digital technologies to connect passengers to drivers who use their personal vehicles to provide for-hire ride services." Texas A & M Transportation Institute , Transportation Policy Research Center, *Policy Implications of Transportation Network Companies – Final Report* at 3 (PRC 17-70F, October 2017)(hereinafter "*Texas A&M")* available at https://policy.tti.tamu.edu/congestion/policy-implications-of-transportation-network-companies/ As of August 2017, 48 states and Washington, D.C. have enacted at least one law regulating some aspect of a Transportation Network Company. *Id.* at 3.

[269]. The question of what level of government should regulate Platform Services is an open debate. While frequently perceived as being a local issue, as discussed in Footnote !4 the TNCs have found that there is an advantage to have regulation at the State level. Some have argued that in the United States the federal government should assume an active role in the regulation of Platform Services in some areas, for example, enforcement of national anti-discrimination laws and the protection of consumers (both consumers and service providers) so as to work with state and local governments in determining what policy approaches are most successful. *See, Light, The Role of the Federal Government in Regulating the Sharing Economy, Forthcoming, 2018* in CAMBRIDGE HANDBOOK ON THE LAW OF THE SHARING ECONOMY (Nestor Davidson, Michèle Finck, and John Infranca, eds., Cambridge Univ. Press), chapter available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047322. A similar debate is occurring in such IoT technologies as autonomous vehicle standards and testing.

[270]. *Id.*, at 30 – 34. A majority of state legislation pre-empt at least some of the local regulation of TNCs, *Id.* at 31. This primarily reflects a state-level policy of promoting the growth of TNC services, as opposed to the actual regulation of TNC services. Specifically, taxi services are generally regulated and enforced at a local level. By pre-empting local regulation of TNCs, the industry avoids the need of fighting definitional legislative battles over what the actual service is on a piecemeal basis.

why it exists. In some markets, regulation has been adopted to both control market entry and market capacity, thus establishing a stable market environment.

Thus, in addition to addressing issues of consumer protection, another reason why regulators seek to determine the regulatory definition of Platform Service providers is to accommodate the disruptive effect that these new providers have on market economic conditions. The fact that regulators decide to adopt different regulatory schemes for similar services is frequently a matter of political discretion of the governing legislative body. That does not mean that existing competitors will not seek to challenge the definition of Platform Services as being regulatory hybrids.

The fact that legislators have adopted differing regulation for what many perceive to be similar services has been upheld by the courts. For example, in a 2016 decision the United States Court of Appeals for the Seventh Circuit found that platform services ride sharing companies were different than taxi companies and could be subject to different regulations.[271] The taxi companies had brought suit alleging that the value of their businesses were declining in violation of their constitutional rights. They argued that the platform services with whom they were competing were engaging in anticompetitive actions, in part due to the fact they operated under less strict regulatory standards. However, the appellate court refused to accept the argument that ride sharing platform services were the same as traditional taxis:

> The plaintiffs argue that the City has discriminated against them by failing to subject Uber and the other TNPs to the same rules about licensing and fares (remember that taxi fares are set by the City) that the taxi ordinance subjects the plaintiffs to. That is an anticompetitive argument. Its premise is that every new entrant into a market should be forced to comply with every regulation applicable to incumbents in the market with whom the new entrant will be competing.
>
> Here's an analogy: Most cities and towns require dogs but not cats to be licensed. There are differences between the animals. . . . Dog owners, other than those who own cats as well, would like cats to have to be licensed, but do not argue that the failure of government to require that the "competing" animal be licensed deprives the dog owners of a constitutionally protected property right, or alternatively that it subjects them to unconstitutional discrimination. The plaintiffs in the present case have no stronger argument for requiring that Uber and the other TNPs be subjected to the same licensure scheme as the taxi owners. Just as some people prefer cats to dogs, some people prefer Uber to Yellow Cab, Flash Cab, Checker Cab, et al. They prefer one business model to another. The City wants to encourage this competition, rather than stifle it as urged by the plaintiffs, who are taxi owners. [272]
>
> * * *
>
> There are enough differences between taxi service and TNP service to justify different regulatory schemes, and the existence of such justification dissolves the plaintiffs' equal protection claim. Different products or services do not as a matter of constitutional law, and indeed of common sense, always require identical regulatory rules. The fallacy in the district judge's equal protection analysis is her

[271]. *Illinois Transp. Trade Ass'n v. City of Chicago,* 839 F.3d 594, 598 (7th Cir. 2016).
[272]. *Id.,* at 597-598.

> equating her personal belief that there are no significant differences between taxi and TNP service with the perception of many consumers that there are such differences—a perception based on commonplace concerns with convenience, rather than on discriminatory or otherwise invidious hostility to taxicabs or their drivers. If all consumers thought the services were identical and that there was therefore no advantage to having a choice between them, TNPs could never have gotten established in Chicago. [273]

Defining the Regulatory Need

The questions of public safety; consumer protection; and responsibility for liability are several of the underlying reasons why regulators seek to determine whether a Platform Service is a traditional or new type of business. Regardless of whether a Platform Service is defined as a traditional business entity, such as a taxi service, or something new, such as a TNC, the underlying regulatory issue is whether there is a need to protect the public.

Defining the need for regulation starts with the initial analysis of defining the nature of the product or service. As discussed, the inquiry may be complete if in defining the service the regulator utilizes an analysis similar to that employed by the European Court of Justice or the UK Tribunal in their *Uber* decisions and find nothing more than a traditional service that is already regulated.

However, determining regulatory need and how to regulate is more difficult if the Platform Service is defined as being a hybrid or new service. The inquiry then shifts to the role of each party to the Platform services transaction, rather than focusing on the nature of the overall service provided.

In the case of Platform Services in the "Sharing Economy", this requires a determination of the role of (a) the consumer, (b) the Platform, and (c) the individual service provider, who may be an individual rather than a business. As with a square peg in a round hole, the question for regulators is whether the hybrid service and the role of each participant (1) creates a regulatory need and, if so, (2) whether the existing regulations apply to the parties to the new service.

The OECD cites the example of the European Union's Consumer's Rights Directive to illustrate this regulatory definitional problem:

> In the European Union, the Consumer Rights Directive applies "to any contract concluded between a trader and a consumer" [Art. 3 (1)]. In other words, it does not apply to contracts between two traders, two consumers or two peers. The Directive defines a "consumer" as any natural person who is "acting for purposes which are outside his trade, business, craft or profession" [Art. 2 (1)].[9] By contrast, a trader is defined as 'any natural person or any legal person, …, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive'(Art. 2 (2) Consumer Rights Directive). The key question under EU law is under which conditions does a peer who rents out her apartment or offers to cut hair or share a bike does so within or outside her trade, business, craft or profession. This is a difficult question for which comprehensive guidance is

[273]. *Id.,* at 598-599.

> lacking. Factors that can matter in this decision vary from country to country (Helberger, et al., 2013: 42). Possible factors include whether a transaction is planned or not, the way it is organised, the number of transactions, their value, the duration of the activity, the impression to the outside world, the way the activity is perceived by consumers, and commercial intentions.[274]

Academics and government regulators are just beginning to explore the legal issues related to these disruptive business models when they are hybrids that do not fit into regulatory models and definitions for existing business models.[275] Consensus has not emerged on whether regulation is needed, let alone how to regulate. Determining who is responsible for liability issues when things go wrong resulting in injury, either to the consumer or to third parties, is also not resolved.

In the absence of regulation, one approach to addressing the potential legal issues inherent in new business models is to educate the public as to existing risks in using the new services. Thus, the National Association of Insurance Commissioners has issued guidelines on insurance implications of home sharing services. It has also issued insurance principles for legislators and regulators related to TNCs.[276]

A second approach is the possibility of industry self-regulation, perhaps with industry codes of conduct, accountability measures, and enforcement mechanisms operating as an effective substitute for traditional consumer protection laws and regulatory oversight.[277]

A third approach is for the Platform Service providers to work with others to develop model legislation that can be enacted by legislators so as to establish a preferred regulatory scheme. This approach, reflected by the TNC legislative model, has the advantage of allowing hybrid services be recognized as a new type of business entity, with perhaps a type and level of regulation that the new business is comfortable with.[278] It also has the advantage of avoiding piecemeal fights at a local level over the very definition of the new business. However, as reflected by the "dogs and cats litigation", it does not prevent established businesses from

---

[274]. OECD, *Protecting Consumers in Peer Platform Markets,* OECD Digital Economy Papers No. 253 at 20 (2016).

[275]. *See, e.g.,* Miller, *First Principles for Regulating the Sharing Economy*, 53 Harvard Journal on Legislation 147 (2016); Jones, *Share and Share Dislike: The Rise of Uber and AirBNB and How New York City Should Play Nice,* 24 Journal of Law and Policy 204 (2016); Munkøe, *Regulating the European Sharing Economy: State of Play and Challenges*, 52 Intereconomics, 38 (2017); Cannon and Chang, *A framework for Designing Co-Regulation Models Well-Adapted to Technology – Facilitated Sharing Economies*, 31 Santa Clara Computer & High Tech. L.J. 23 (2014); Rauch and Schleicher, *Like Uber, but for Local Government Law: The Future of Local Regulation of the Sharing Economy*, 76 Ohio St. L.J. 901 (2015); Lobel, *The Law of the Platform*, 101 Minn. L. Rev. 87 (2016); Stemler, *Betwixt and Between: Regulating the Shared Economy,* 43 Fordham Urb. L.J. 31 (2016).

[276]. National Association of Insurance Commissioners (NAIC), Transportation Network Company *Insurance Principles for Legislators and Regulators* (2016); NAIC, *Insurance Implications of Home-Sharing: Regulator Insights and Consumer Awareness* (2016).

[277]. OECD, *Protecting Consumers in Peer Platform Markets,* OECD Digital Economy Papers No. 253 at 5 (2016).

[278]. For example, TNC legislation can be categorized into seven broad policy areas: permits and fees; insurance and financial responsibility; driver and vehicle requirements; operational requirements; passenger protections; data reporting; regulatory and rule-making authority. *Texas A & M, supra*, note 12, at 18.

challenging the new market disrupters. It also does not necessarily address criticisms that an insufficient level of regulation has been enacted.[279]

Can Algorithms and Data Analytics Replace the Need for Traditional Regulation?

If a Platform Service is a new hybrid business model, the question of what type of regulation is appropriate for the new business depends, in part, on the perceived risk of market participant abuses. This, in turn, requires an analysis of whether the use of computer algorithms and data analytics as core functions of a Platform Services business will either lessen or increase the need for regulation. In some cases, it may be both.

In November 2016, the Federal Trade Commission published the results of a workshop it held on the Platform economy.[280] Its discussions included the various ways in which Platform companies seek to define themselves and their services, as well as the ways in which Platform services may need to assume responsibility to the public.

Platform services involve the provision and consumption of services by and between strangers. How to protect the public when strangers perform services for other strangers is one of the key issues regarding the liability and possible need to regulate Platform Services and the Sharing Economy. As the FTC noted, the regulation of service providers frequently reflects public policy determinations involving issues of public safety; consumer protection; insurance and liability; employment rights; civil rights and anti-discrimination laws; the promotion of market efficiency and common laws; and government finances (in the form of tax collection).[281]

Platform Service providers frequently argue many of these issues are actually a "trust" issue. They argue that their data analytics and rating apps can create trust in consumers about using their services that can be a substitute for more traditional forms of regulation.[282]

For example, traditional taxi companies are often required to conduct government-mandated driver criminal background checks; the inspection of vehicles; and maintain

---

[279]. Driver background checks and insurance requirements are two examples of such criticism. Traditional taxi companies are frequently required to conduct fingerprint and criminal background checks of their drivers. TNCs, by way of contrast, frequently rely on commercial background checks and seek to eschew fingerprinting. *Texas A & M, supra*, note 12, at 38-43. With respect to insurance issues, there is a question as to whether the levels of mandatory insurance coverage are adequate to protect the public. For example, under the California TNC statute and regulations, there are three different levels of insurance that may apply with respect to the TNC and its driver. In Period 1 the driver has the App open and is waiting for a match. The TNC is required to provide primary insurance in the amount of at least $50,000 for death and personal injury per person; $100,000 for death and personal injury per indent; and $30,000 for property damage. In Period 2 the driver and customer have accepted a match and the passenger has not yet been picked up. Period 3 is when the passenger is in the vehicle. In Periods 2 and 3 the TNC must provide primary commercial insurance of $1 million and, in Period 3 it must also provide uninsured and underinsured motorist coverage in the amount of $1 million. *See,* California Public Utilities Commission, *Insurance Requirements for TNCs; http://www.cpuc.ca.gov/General.aspx?id=3802. Also see, California Public Utilities Code Article 7 – Transportation Network Companies.* Critics of the different levels of liability argue that a driver looking for a ride should be considered as driving for the TNC and that a higher level of insurance coverage should be required.

[280]. FTC, *The "Sharing" Economy: Issues Facing Platforms, Participants & Regulators* (Nov. 2016).

[281]. *Id.*

[282]. *Id.* at 30-50.

mandatory levels of insurance so that the public has a uniform level of assurance that the taxi they hail on the street with a stranger driver meets a minimum level of uniform safety standards.

Ride sharing Platforms or TNCs, on the other hand, argue that while they do perform driver background checks, they do not need to comply with the stricter regulatory standards required of taxi companies because their computer applications allow their customers to provide a rating of drivers and vehicles. These ratings, they argue, supplement their less stringent background checks to allow the public to make their own decisions on whether a driver and vehicle are safe due to their reputation in the platform community. In other words, market information will create public safety in the services they provide.[283]

Whether customer data supplemented by computer algorithms should replace other forms of regulatory consumer protections is an open question. Some studies have noted that consumers trust peer Platform Services over traditional businesses.[284] However, the FTC Report noted that while Platform companies tout the benefits of their ratings apps as a way to screen service providers, such screenings can be imperfect and prone to bias and manipulation.[285] In addition, third parties and the general public who may be injured as a result of the provision of a Platform Service may not be able to rely on the Platform's data analytics and algorithms to address issues related to the public safety of such services.[286] The OECD has noted that trust and reputation systems can also invite discrimination.[287] In addition, the fact that Platform companies must take adequate measures to protect the data and privacy of their customers and service providers can, in some circumstances, limit the availability of information that is shared with consumers.

Do Algorithms and Data Analytics Increase the Need for Regulation?

In other areas, experience points to the fact that the ability to control and manipulate data may require more regulation of Platform Services, not less. Legal issues related to data privacy, cyber-security, law compliance, and competition law issues have all been raised in connection with Platform Services and their regulation.

For example, in late 2017 Uber was denied a renewal of its private hire operator license by Transport for London (TfL) due to "a lack of corporate responsibility in relation to a number of issues which have potential public safety and security implications."[288] One of the issues upon which TfL based its decision to deny renewal of Uber's license was on Uber's "approach to explaining the use of Greyball in London." Greyball was a software algorithm that TfL explained "could be used to block regulatory bodies from gaining full access to the app and prevent

[283]. Ways by which a Platform Service may build consumer trust is by establishing review and reputation systems; guarantees or insurance; verified identities; pre-screening of providers and consumers; secure payment systems; and education, checklists, and forms. OECD, *Protecting Consumers in Peer Platform Markets,* OECD Digital Economy Papers No. 253 at 17, 18 (2016).

[284]. OECD, *Trust in Peer Platform Markets,* OECD Digital Economy Paper No. 263 at 26 (November 2017).

[285]. *FTC Report* at 40-42.

[286]. *Id.* at 81.

[287]. OECD, *Protecting Consumers in Peer Platform Markets,* OECD Digital Economy Papers No. 253 at 19 (2016).

[288]. Press Release, Transport for London, Licensing Decision on Uber London Limited (Sept. 22, 2017), https://tfl.gov.uk/info-for/media/press-releases/2017/september/licensing-decision-on-Uber-london-limited. Uber's appeal of the TfL decision is still pending as of June 2018.

officials from undertaking regulatory or law enforcement duties."[289] Other commentators have suggested that Greyball could be used to discriminate against certain neighborhoods or ethnicities.[290]

In the United States, Uber has been challenged on a variety of fronts with respect to its data-related business practices. One challenge involved an August 2017 settlement of a FTC complaint relating to Uber's use of its "'God View'" software.[291] In that complaint, the FTC alleged that Uber misrepresented to consumers the extent to which it monitored its employees' access to personal information about users and drivers.[292] It also complained that Uber misrepresented to consumers how it secured data about users and drivers.[293] In settling the complaint with the FTC, Uber was prohibited from misrepresenting how it monitors internal access to consumers' personal information and how it protects and secures data.[294] Uber also agreed that it would implement a comprehensive privacy policy that addresses privacy risks related to "new and existing products and services," and that "protect[s] the privacy and confidentiality" of personal data collected by the company.[295] It further agreed that for the next twenty years it would obtain, every two years, an independent third-party audit certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC's order.[296]

In addition to data privacy and cybersecurity issues competition law issues may also require regulation of Platform Services. As previously discussed, existing businesses faced with competition from new market entrants have challenged the application of different regulatory standards to such services when the underlying service appears to be the same. One of the regulatory challenges in assessing whether new market entrants using a new technology need to be regulated is determining their effect on existing market participants and related competition.

Regulators do recognize that the compilation and use of big data can also present competition law concerns. Price signaling; price calculation; and other forms of restriction on competition may be facilitated by computer analytics.[297] Whether algorithms need regulatory approval is a topic that is being discussed.[298] As the Transport for London *Uber* decision

---

289. *Id.*

290. *Uber's Secret Program Raises Questions About Discrimination*, The Atlantic, March 3, 2017; https://www.theatlantic.com/technology/archive/2017/03/uber-ghost-app/518610/

291. Federal Trade Commission, *In the Matter of Uber Technologies, Inc., Agreement Containing Consent Order*, File No. 1523054 (August 15, 2017); FTC, *Uber Technologies, Inc; Analysis to Aid Public Comment,* 82 Fed. Reg. 39582 (Aug. 21, 2017). ["Analysis"]

292. *Id.*

293. *Id.*

294. *Id.*

295. *Id.*

296. *Id.*

297. *See, e.g., Meyer v. Kalanick,* 174 F.Supp. 3d 817 (S.D. N.Y. 2016), in which the court refused to dismiss an antitrust claim against the CEO and founder of Uber alleging that the defendant "while disclaiming that he was running a transportation company, had conspired with Uber drivers to use Uber's pricing algorithm to set the prices charged to Uber riders, thereby restricting price competition among drivers to the detriment of Uber riders", such as the plaintiff. An evaluation and ruling on this issue will not occur, because a subsequent appellate court decision required the case to proceed to arbitration.

298. *See, Algorithms and Coordinated Effects*, Remarks of Federal Trade Commissioner Terrell McSweeny, University of Oxford Center for Competition Law and Policy (May 22, 2017), available at https://www.ftc.gov/public-statements/2017/05/algorithms-coordinated-effects.

demonstrates, the use of algorithms has already resulted in regulatory actions affecting the ability of at least one Platform Services company to provide its services.

In the future the use of data by Platform Services in the sharing economy is thus likely to increase, not decrease, as an area of regulatory concern. This will happen even if the actual services provided by the Platform Services provider is not regulated. Implementation of the EU General Data Protection Regulation ("GDPR") and similar laws guarantees that the data privacy and cyber-security aspects of Platform Services business models will continue to be regulated, at least for companies whose operations are within the scope of the applicable regulation.[299]

In addition, even without the GDPR and similar statutes government investigations of data breaches involving Platform Services are likely to result in changed business practices, if not greater regulatory scrutiny, of these businesses.

For example, in November 2017, Uber announced that it had concealed an October 2016 data breach involving "the theft of personal information from" at least "57 million user accounts and 600,000 US drivers."[300] The delayed report of the hacking of Uber's computer systems resulted in investigations being opened by regulators in various states and countries, including investigations by the Federal Trade Commission, the New York Attorney General, the United Kingdom's Information Commissioner's Office, and the UK National Cyber Security Centre.[301] Such investigations are warnings to all companies that regulatory oversight of data use and security will only increase in the future. Whether it will result in new regulations, or the application of existing regulations, remains to be seen.[302]

Should the Platform Services Contracting Terms be Regulated?

Even if algorithms and data analytics can solve the consumer trust issue, the business practices of Platform Service providers raise other regulatory issues that may require government oversight, especially in their contracting practices.

One of the premises of the Sharing Economy is that the Platform Service is an intermediation tool that allows individual service providers acting as independent contractors to provide individual services to consumers. However, since the Platform is the foundation of the underlying business model and crucial to its utilization, the Platform Service provider has the economic power and ability to mandate contractual terms and conditions that may give it a favored position with respect to both the consumer and the independent service provider. This could include limitations on its own responsibility or liability for services provided via use of the platform. The Platform Service could also require mandatory or non-negotiable terms and

[299] *Regulation (EU) 2016/679 of the European Parliament and of the Council 27* April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[300] Michael Kan, *Uber Faces Regulatory Scrutiny for Concealing Data Breach,* PC Magazine (Nov. 22, 2017), https://www.pcmag.com/news/357528/uber-faces-regulatory-scrutiny-for-concealing-data-breach

[301] *Id.*

[302] Reilly, K., *Data, the Sharing Economy and Canadian Federal Regulation*, Medium, (February 16, 2018), published at https://medium.com/@kmareilly/canadian-federal-government-regulation-data-and-the-digital-platform-economy-22da446f0dc4

conditions of the other parties using the service, including the consumer and the actual services provider.[303]

The fact that a Platform Service provider uses its contracts to define the individual service provider as being an independent contractor, does not prevent regulators or the courts from examining the circumstances surrounding the relationship and ruling that the contractual definition is not legally accurate or does not meet the public good.

As indicated in the UK Employment Tribunal *Uber* decision, regulators examining the relationships between Platform Service providers and their contract parties may choose to return to the initial question of how the overall service is defined and simply ignore or even dictate how the Platform Service contractually self-defines its relationships with consumers and service providers.

In other circumstances, regulators may decide that Platform Service providers are the parties with sufficient economic power and resources that such issues as imposing responsibility for insurance and tax collection and remittance requires a legislative solution imposing such obligations on the Platform Service, not the other parties to the transaction., who may lack economic resources, means, or knowledge to meet such obligations.[304]

In the absence of regulatory solutions, the courts ultimately will be asked to determine whether Platform Services contracts are enforceable or subject to generally applicable laws. Ride sharing companies have experienced and settled numerous lawsuits from drivers claiming that notwithstanding the mandatory terms and conditions required by the Platform they are not independent contractors but are actually employees of the company, entitled to certain rights and benefits under the law.

In a similar manner, determining such issues as who is responsible when the provided services injure a third party, the courts, at least in the United States, may look to common law standards of liability based both on the contractual definitions that the Platform Services provider has dictated as applying between the parties who performed the services and those who facilitated them, as well as general rules of social responsibility in determining whether the Platform Service should, in fact, be the responsible party for third party liability claims related to the services it help facilitate. Examples include concepts of vicarious liability based on the theory that as the party facilitating the service, and the economic ability to bear the loss, the Platform should be held responsible for injuries and loss that occur during the performance of services that it has facilitated.[305]

---

[303] The question of how to achieve fairness between all parties to Sharing Economy transactions is an area of increasing concern to academics and policy makers. *See, e.g.,* Newland, Lutz, and Fieseler, *Recommendations for the Sharing Economy: (Re-)Balancing Power, Report* from the EU H2020 Research Project Ps2Share: Participation, Privacy, and Power in the Sharing Economy (2018) available at https://brage.bibsys.no/xmlui/handle/11250/2483317.

[304] Munkøe, *Regulating the European Sharing Economy: State of Play and Challenges,* 52 Intereconomics 38 (2017). Katz, *Regulating the Sharing Economy,* 30 Berkeley Technology Law Journal 1067 (2015).

[305] *See, e.g.,* Geisser, *Risk, Reward, and Responsibility: A Call to Hold UberX, Lyft, and Other Transportation Network Companies Vicariously Liable for the Acts of Their Drivers,* 89 S. Cal. L. Rev 317 (2016); Sachs, *The Common Carrier Barrier: An Analysis of Standard of Care Requirements, Insurance Policies, and Liability Regulations for Ride-Sharing Companies*, 65 DePaul L. Rev. 873 (2016); Pfeffer-Gillett, *When "Disruption" Collides with Accountability: Holding Ridesharing Companies Liable for Acts of their Drivers,* 104 Calif. L. Rev. 233 (2016).

Conclusion

With respect to Platform Services and the Sharing Economy, the debate over whether the Fourth Industrial Revolution will require more or less governmental regulation is one that has already started.

One of the most compelling arguments against industry regulation is the need to provide innovative businesses the room and flexibility to explore new ways of doing business. It is a compelling argument to allow Platform Services to continue exploring new ways to harness new technologies to provide more competitive business services.

At the same time, traditional regulatory schemes frequently establish liability and insurance requirements for regulated industries so that both businesses and consumers have some predictability in determining both the risk in using the service as well as whether the party providing the service has sufficient insurance to pay for the loss. Similarly, industries are sometimes regulated so that communities can manage competition issues related to supply and demand, so that industries can effectively function in providing a common need. Industry disruption is often a good thing, but sometimes you can have too much of a good thing.

The legal and regulatory issues related to the introduction of Platform Services and the disruption they have created in many industries will eventually be resolved. How they are resolved will either be through litigation seeking to define where these services fit in the existing regulatory scheme or through the political and legislative process, by the adoption of new laws that establish a new category of services. Regardless of how these issues are resolved, by forcing a re-examination and reconsideration of the law applicable to their services these disruptive technologies and businesses may also require a disruption in existing laws.

About the Author

Andrew M. Danas (adanas@gjcobert.com) is a Partner with Grove, Jaskiewicz, and Cobert LLP, in Washington, D.C. A frequent speaker on business matters related to international commerce, Andrew publishes regularly in professional and academic journals. He is also active in a number of professional organizations in a leadership capacity. Andrew currently serves as Co-Chair of the International Transportation Committee of the American Bar Association Section on International Law; Co-Chair of the Antitrust and Unfair Trade Practices Committee of the Transportation Lawyers Association; and Secretary and Management Committee Member of the Euro-American Lawyers Group.

He is Member of Euro-American Lawyers Group; Secretary and Member of Management Committee of the Transportation Lawyers Association; Co-Chair, Antitrust and Unfair Practices Committee; American Bar Association Section of International Law; Co-Chair, International Transportation Committee (2014-2017); American Bar Association Section of International Law; Vice-Chair, International Contracts Committee (2017-2018).

Mr. Danas is a member of the District of Columbia Bar. He is also admitted to practice in the following federal courts: Supreme Court of the United States, U.S. Court of Appeals for the District of Columbia Circuit, the U.S. Court of Appeals for the Second, Third, Fourth, Sixth, Eleventh, Federal Circuits, for the U.S. District Court for the District of Columbia, the U.S. Court of International Trade, and the U,S, Court of Federal Claims.

Discussion Questions

1. In addition to introducing new ways of doing business, these new products and services bring with them corresponding questions of regulation and liability. If rules are required, should existing rules be used or is a new regulatory template required?

2. Should these innovative businesses be left free from Regulations, in order to allow flexibility and to continue exploring new ways to harness new technologies to provide more competitive business services?

3. Or should these industries be regulated so that both businesses and consumers have some predictability in determining the risk in using the service as well as whether the party providing the service has sufficient insurance to pay for the loss?

4. Should these decisions be made through the political and legislative process or through piecemeal litigation?

To Cite this Article

Danas, A. M. (2018, Fall). Disruptive technologies and business models: Emerging regulatory issues from the sharing economy. *Journal of Multidisciplinary Research, 10*(3), 45-60.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 61-80.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

The Internet of Things: Insurance Coverage Considerations

Ellen M. Farrell
Crowell & Moring

and

Rachel P. Raphael*
Crowell & Moring

Abstract

The article begins exploring the improvements that still are to be made in the techniques used to secure IoT devices, especially in view of the vulnerabilities that led to lawsuits against companies involved in the production, sale, distribution, and marketing of Internet-connected products. These complicated risks generate complicated insurance issues.

After briefly discussing the background of risks associated with IoT devices, their regulation and litigation, this article discusses how courts and the Insurance Services Office (ISO) have considered coverage for other cyber-related incidents and what these court decisions might suggest for coverage issues that arise concerning IoT devices. In particular, the article explores IoT risks, federal regulation and litigation, and risks to privacy, cybersecurity, and safety.

Addressing Federal Regulation, the article supplies information from the U.S. Department of Commerce (DOC), the National Telecommunications and Information Administration (NTIA), the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), the National Highway Traffic Safety Administration (NHTSA), the Federal Communications Commission (FCC), the U.S. Department Homeland Security (DHS), the U.S. Department of Justice (DOJ), the U.S. Department of Defense (DOD), the National

* The authors thank Tom Kinney, Anupama Prasad, and Sahar Sabir for their assistance with this article.

Science Foundation (NSF), the National Aeronautics and Space Administration (NASA), the National Institutes of Health (NIH), and the U.S. Department of Veterans Affairs (VA).

The article then moves to exploring present and expected litigation, referencing the class action lawsuits that were filed against automobile manufacturers over alleged vulnerabilities in the computer systems used in "connected" cars.

Finally, the article covers the specific issues of insurance coverage, reporting on cases that define "property damage" in the IoT context, unauthorized use of data under "traditional" liability policies, such as data breaches and advertising injury.

The article then switches to ISO endorsements, to "stand-alone" Cyber Policies, and to general IoT coverage issues.

The article concludes that in relation to IoT products, being susceptible to attacks, there will be a next wave of insurance coverage litigation, so that insurance carriers and policyholders should pay careful attention to the specific terms of their insurance policies to make sure the available coverage satisfies both parties' expectations.

Introduction

Today, billions of different devices are connected to the Internet and the Internet-capability of everyday objects is expected to grow exponentially in the years to come. The Internet of Things (IoT) refers to the network of these devices that collect and exchange data. Connected devices may include everything from automobiles to implantable medical devices to home appliances. The large-scale use of these devices is already revolutionizing many aspects of our daily lives by increasing the availability of information and changing the ways that business and consumers interact. However, at the same time, it is creating a host of new cyber-related risks, as a wealth of new information may be open for attack.

Indeed, controlled demonstrations and data breach incidents have shown that there are still improvements to be made in the techniques used to secure IoT devices. The exposure of vulnerabilities has led to lawsuits against companies involved in the production, sale, distribution and marketing of Internet-connected products. When facing potential liability, companies commonly turn to their insurance policies for coverage. However, with complicated risks come complicated insurance issues. The tangible and intangible nature of data breaches involving IoT products raises interesting issues under both stand-alone cyber insurance and more traditional liability policies. After briefly discussing the background of risks associated with IoT devices, their regulation and litigation, this article discusses how courts and the Insurance Services Office (ISO) have considered coverage for other cyber-related incidents and what these court decisions might suggest for coverage issues that arise concerning IoT devices.

I. IOT Risks, Federal Regulation, and Litigation

IoT is generally understood to refer to a decentralized network of physical objects that are connected to the Internet and enable communication between humans, computers, objects, applications and devices.[306] The number of connected objects in the IoT is growing at a rapid

[306] Nasrine Olson, *The Internet of Things*, 18 New Media & Soc'y 680 (2016) (book review); National Sec. Telecomms. Advisory Comm., NSTAC Report to the President on the Internet of Things (2014).

rate: In 2003, approximately 500 million devices were connected to the Internet.[307] Today, there are over 6.4 billion such devices, with approximately 5.5 million more connecting to the Internet each day.[308] By 2020, the number of devices in the IoT is predicted to exceed 20 billion[309] -- possibly reaching as much as 40 to 50 billion.[310]

A. Risks

The IoT presents risks to privacy, cybersecurity and safety. As to privacy, within the IoT, billions of sensors around the world are constantly acquiring information about their surroundings, and new ways of capturing and using personal information continue to emerge.[311] As a result, there are concerns regarding the unpermitted access to and misuse of personal information and consumer data[312]; for example, data collected from the IoT might be used in ways its consumers did not authorize.[313] Another privacy concern is the ease with which hackers may conduct identity theft: "General data available on the internet, combined with social media information, plus data from smart watches, fitness trackers and if available smart meters, smart fridges and many more" provide hackers with "a great all-round idea" of individual identities.[314]

As to cybersecurity, the potential of cyber-attacks (and associated costs) has risen, and will continue to rise, with the growing number of smart objects in the IoT. Cybersecurity is designed to protect "information systems, their components and contents, and the networks that connect them from intrusions or attacks involving theft, disruption, damage or other unauthorized or wrongful actions."[315] Cyberattacks result not only in the theft of data but also can cause bodily injury and property damage.[316] For example, in 2008, hackers accessed a Turkish Pipeline through surveillance camera software and caused an explosion by super-pressurizing the oil in the pipeline after shutting down its alarms.[317] In 2014, the German Federal Office of Information Security announced that hackers had gained access to a German steel factory's production networks and caused system components to fail by tampering with the controls of its blast furnace.[318] More recently, in January 2017, hackers infiltrated an Austrian

[307] Shawn DuBravac & Carlo Ratti, The Internet of Things: Evolution or Revolution? 6 (2015).

[308] H. Michael O'Brien, *The Internet of Things and its Future Impact on Product Liability* (2015).

[309] *Id.*

[310] DuBravac & Ratti, *supra* note 2, at 2.

[311] DuBravac & Ratti, *supra* note 2, at 15.

[312] Mohana Ravindranath, *Who's in Charge of Regulating the Internet of Things?,* Nextgov (Sept. 1, 2016), http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/.

[313] *Id.*

[314] Lea Toms, *Beware! Data and Identity Theft in the IoT*, GlobalSign Blog (Mar. 22, 2016), https://www.globalsign.com/en/blog/identity-theft-in-the-iot/.

[315] Eric A. Fischer, Cong. Research Serv., R44227, The Internet of Things: Frequently Asked Questions 14 (2015).

[316] *Id.*

[317] Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar,* Bloomberg Tech. (Dec. 10, 2014, 5:00 AM), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[318] *Hack Attack Causes 'Massive Damage' at Steel Works*, BBC (Dec. 22, 2014), http://www.bbc.com/news/technology-30575104; Andrew Roth, *Not Just the DNC: Five More Hacks the West Has Tied to Russia*, Wash. Post (June 15, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/not-just-the-dnc-five-more-hacks-the-west-has-tied-to-russia/?utm_term=.d0fd4b683b32.

hotel's electronic key system, locking guests out of their rooms and forcing the hotel to give in to the hacker's ransom demand.[319] And just eight days before President Trump's inauguration, hackers tampered with 70% of storage devices that record data from police surveillance cameras in Washington, D.C., "forcing major citywide reinstallation efforts."[320]

Finally, the most significant risk posed by IoT is the risk to our safety – by, for example, the unauthorized access to medical devices. For instance, in 2014, the Federal Bureau of Investigation (FBI) warned hospitals to discontinue use of a particular line of infusion pumps produced by Hospira due to security flaws that could allow a user to change remotely medication doses.[321] In addition, in January 2017, the Food and Drug Administration (FDA) confirmed that St. Jude Medical's implantable cardiac devices had vulnerabilities that could allow a hacker to access them and deplete their batteries or administer incorrect pacing or shocks, or both.[322]

Hackers can also endanger our safety by targeting different modes of transportation. For example, in 2008, a teenage boy hacked into a Polish train system, causing a train derailment and injuring at least 12 people.[323] In April 2015, the U.S. Government Accountability Office (GAO) published a report addressing cybersecurity issues with commercial aircraft.[324] In its report, the GAO noted that the increasing interconnectedness of modern aircraft creates the possibility of unauthorized access to aircraft avionics systems.[325] Similarly, "[w]hile there have been no known cyber-attacks against vehicles . . . most experts believe 'real-world attacks with safety implications could occur in the near future, particularly as automakers begin deploying autonomous (i.e., self-driving) vehicles and connected vehicle technologies.'"[326]

B. Federal Regulation

As with any new, emerging technology, both public and private sectors are struggling to keep up with the IoT and its rapidly advancing role in everyday life. Most IoT regulation consists

---

[319] Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, N.Y. Times, Jan. 30, 2017, https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0.

[320] Clarence Williams, *Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose*, Wash. Post, Jan. 27, 2017, https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.7ccd6a0e1b23.

[321] Jessica Condit, *FDA Tells Hospitals to Ditch IV Pumps That Can be Hacked Remotely*, Engadget (July 31, 2015), https://www.engadget.com/2015/07/31/fda-security-warning-hackers/.

[322] Press Release, FDA, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication (Jan. 9, 2017).

[323] Graeme Baker, *Schoolboy Hacks into City's Tram System*, Telegraph (Jan. 11, 2008), http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

[324] U.S. Gov't Accountability Office, GAO-15-370, Air Traffic Control – FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen (2015).

[325] *Id*.

[326] *See* Paul Merrion, "House smart car caucus revs up vehicle cybersecurity issue," Congressional Quarterly Roll Call (April 28, 2016). The possibility of such intrusions was confirmed in mid-2015 when two individuals conducting a "white hat" hacking experiment were able to manipulate systems and then disable a Sport Utility Vehicle speeding on a busy highway 10 miles away. Michael E. Miller, *'Car Hacking' Just Got Real: In Experiment, Hackers Disable SUV on Busy Highway*, Wash. Post, July 22, 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/?utm_term=.7a30e09871f9.

of guidance or non-binding principles various federal agencies suggested (although Sates are beginning to weigh in as well).

There is no single federal agency with oversight of the IoT – instead, multiple different agencies each have sector-specific regulatory responsibility for the IoT.[327] For example, within the U.S. Department of Commerce (DOC), in 2014 the National Institute of Standards in Technology (NIST) unveiled a cybersecurity framework for identifying cybersecurity vulnerabilities, and putting practices and procedures in place to minimize them, detecting breaches and responding to them.[328] Although not specific to the IoT, the NIST framework certainly encompasses the IoT, and other federal agencies have referenced the NIST framework when suggesting best practices with respect to cybersecurity and IoT for entities that they regulate. Separately, the National Telecommunications and Information Administration (NTIA) recently issued "Fostering the Advancement of the Internet of Things," a Green Paper representing the DOC's analysis of public comments received on the current technological and policy IoT landscape in 2016.[329]

In January 2015, the Federal Trade Commission (FTC), whose mission is to prevent unfair and anticompetitive business practices,[330] issued a Staff Report specific to the IoT.[331] This report describes "best practices" for companies to consider, including a proactive approach to the security of IoT devices,[332] and minimizing the collection and retention of consumer data.[333]

The Food and Drug Administration (FDA) regulates IoT medical devices. The FDA has issued guidance as to the security of such devices, including in December 2016.[334] This guidance encourages implementing a proactive, comprehensive risk management program, and emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities as part of their post-market management of medical devices.[335] It also recommends that manufacturers address security weaknesses by establishing processes handling vulnerabilities,

---

[327] Cong. Research Serv., *supra* note 10 at 9.

[328] *Framework for Improving Critical Infrastructure Cybersecurity,* Nat'l Inst. of Standards and Tech. (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[329] U.S. Dep't of Com., Fostering the Advancement of the Internet of Things (2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[330] https://www.ftc.gov/about-ftc.

[331] U.S. Fed. Trade Comm'n, *Internet of Things – Privacy & Security in a Connected World* 3-4 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[332] *Id.* at iii; *See also* U.S. Fed. Trade Comm'n, Careful Connections – Building Security in the Internet of Things (2015) (the FTC advises companies to encourage a culture of security, implement "security by design", implement a "defense-in-depth" approach, take a risk-based approach, consider the risks of collecting consumer information and avoid using default passwords).

[333] U.S. Fed. Trade Comm'n, *supra* note 26, at iv.

[334] **U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff (2016), https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf. The FDA issued previous guidance in January 2005 and June 2013.**

[335] *Id.*

adopting coordinated vulnerability disclosure policies and deploying strategies to mitigate cybersecurity risk before a cyber-attack takes place.[336]

The National Highway Traffic Safety Administration (NHTSA) within the U.S. Department of Transportation has addressed cybersecurity in vehicles. Recently, the NHTSA issued a "Federal Automated Vehicles Policy," which addresses highly automated vehicles ("HAVs").[337] Among other things, the Policy (1) outlines best practices for the safe pre-deployment design, development and testing of HAVs prior to commercial sale or operation on public roads; (2) establishes a national framework, but leaves states with the responsibilities for vehicle licensing and registration, traffic laws and enforcement, and insurance liability regimes; discusses the NHTSA's available regulatory authority over HAVs including interpretations, exemptions, notice-and-comment rulemaking, and defects and enforcement authority; and identifies new authorities and regulatory structures that could aid deployment of new technologies in a safe and expeditious manner.[338]

Other examples of federal agencies that oversee the regulation of various aspects of the IoT include the Federal Communications Commission (FCC),[339] U.S. Department Homeland Security (DHS),[340] U.S. Department of Justice (DOJ), U.S. Department of Defense (DOD),

---

[336] *Id.*

[337] The National Highway Traffic Safety Administration, Federal Automated Vehicles Policy – Accelerating the Next Revolution In Roadway Safety, (Sept. 2016), https://one.nhtsa.gov/nhtsa/av/av-policy.html.

[338] *Id.*

[339] The FCC recently published "Cybersecurity Risk Reduction," a White Paper on the IoT and reducing cyber risk. *See* U.S. Fed. Commc'n Comm'n, FCC White Paper – Cybersecurity Risk Reduction (2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0118/DOC-343096A1.pdf. In this White Paper, the FCC indicated that cybersecurity was the FCC's top priority, and that the FCC was "uniquely situated to comprehensively address this issue given its authority over the use of radio spectrum as well as the connections to, and interconnections between, commercial networks, which touch virtually every aspect of our economy[.] *Id*. at 4. Among its recommendations, the White Paper called for collaboration with Internet stakeholder groups, cooperation among federal agencies and regulatory solutions where the market fails.

Although former FCC Chairman Wheeler stated that transitioning to a new presidency should not delay the FCC's work towards achieving cybersecurity, the FCC White Paper was rescinded on February 3, 2017, shortly after President Trump was inaugurated. *See* Jenna Ebersole, FCC Claims Role in Internet of Things, Law360 (Jan. 19, 2017), https://www.law360.com/articles/882644/fcc-claims-role-in-internet-of-things-other-cybersecurity; *see* also *In re Pub. Safety & Homeland Sec. Bureau White Paper on Cybersecurity Risk Reduction*, No. DA 17-132 (U.S. Fed. Commc'n Comm'n Feb. 3, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0203/DA-17-132A1.pdf. As such, the White Paper is to have "no legal or other effect or meaning going forward." *Id*. It remains to be seen whether and in what form the FCC may reinstate the White Paper.

[340] On November 16, 2016, DHS released *Strategic Principles for Security the Internet of Things* (IoT) (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. These nonbinding principles, aimed at "stakeholders" with respect to IoT including manufacturers, software developers, and consumers, recommend (inter alia) (1) the incorporation of security at the design phase of IoT devices; managing vulnerabilities in IoT devices, including through security updates; utilizing security practices and prioritizing security based on the potential impact if an IoT device were compromised.

National Science Foundation (NSF), National Aeronautics and Space Administration (NASA), National Institutes of Health (NIH), and the U.S. Department of Veterans Affairs (VA).[341]

C. Litigation

As controlled demonstrations and cyber incidents have begun to expose vulnerabilities in Internet-connected products, courts have started to see litigation involving IoT products. Various parties from individual customers to regulatory agencies have filed these suits, alleging that the susceptibility of these connected products put consumers at risk of bodily injury, property damage and privacy violations. Just as the different types of plaintiffs have run the gamut, so too have the types of devices in question, including over connected cars, children's toys, implantable medical devices, and home security systems.

For example, in 2015, two class action lawsuits were filed against automobile manufacturers over alleged vulnerabilities in the computer systems used in "connected" cars.[342] In *Cahen*, consumers who purchased cars in California, Oregon and Washington filed a putative class action against Toyota, Ford and General Motors alleging that the manufacturers equipped their cars with computer technology that made the vehicles susceptible to hacking and collecting private customer data.[343] According to the complaint, the poor security of the cars' computer systems could cause the driver to lose control of basic functions such as steering, accelerating and breaking and endanger the driver and his or her passengers.[344] The plaintiffs did not allege that their connected cars had been hacked but merely that these cars were *vulnerable* to hacking.[345] As a result, the problem for the plaintiffs in *Cahen* was standing: plaintiffs had to show (1) injury in fact that is "actual or imminent," (2) injury traceable to challenged actions of the car manufacturers, and (3) injury redressable by a favorable judicial decision.[346] The plaintiffs argued they were injured because of the car manufacturers' misrepresentations – had they known about the security issues they would not have purchased their cars or would not have paid as much if they did purchase them.[347] The court was not convinced. The California federal district court dismissed the action for lack of standing, concluding that the alleged risk of hacking was "too speculative" to constitute actual injury.[348] The court also rejected plaintiffs' "benefit of the bargain" argument, explaining that the plaintiffs "have not . . . alleged a demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values."[349]

A month after the class action complaint in *Cahen*, a similar class action complaint was filed against Chrysler and Harmon International seeking damages from alleged security flaws in the "uConnect" systems installed in certain vehicles.[350] Similar to the *Cahen* case, the plaintiffs in *Flynn* alleged that this computer system – which allowed for integrated control of the cars'

---

341 *Id.*

342 *See Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015); *Flynn v. FCA US LLC*, No. 3:15-cv-0855, 2016 U.S. Dist. LEXIS 130614 (S.D. Ill. Sept. 23, 2016).

343 147 F. Supp. 3d at 958.

344 *Id.*

345 *Id.*

346 *Id.* at 965-66.

347 *Id.* at 966.

348 *Id.* at 969.

349 *Id.* at 971. The case is currently on appeal before the Ninth Circuit.

350 *See Flynn*, 2016 U.S. Dist. LEXIS 130614, at *2.

phone, navigation and entertainment functions – contained vulnerabilities that allowed hackers to take remote control of the vehicles steering and braking functions.[351] Plaintiffs' complaint contained a number of causes of action for negligence, fraud, breach of warranty and violations of consumer protection laws.[352] In September 2016, the U.S. District Court for the Southern District of Illinois dismissed or trimmed down plaintiffs' claims, or both.[353] Like the court in *Cahen*, the Illinois federal district court held that the plaintiffs "lack[ed] standing to pursue damages for a risk of harm or a fear of that risk" and dismissed plaintiffs' claims linked to non-economic damages.[354] But unlike *Cahen*, the court in *Flynn* concluded that the plaintiffs had standing to sue for damages concerning the diminished value of their cars given that "ongoing vulnerabilities have reduced the market value of their vehicles."[355]

Another subject of early litigation is connected children's toys. In December 2015, two mothers filed a putative class action lawsuit in California Superior Court against Toytalk and Mattel concerning the companies' Hello Barbie toy.[356] Hello Barbie included a smartphone app that allowed the parents to play, share, and delete the audio recordings of their children produced by the doll.[357] The doll would engage in conversation with the child, record the conversation and then store the recording on the cloud.[358] Among other things, the plaintiffs alleged that the toy was not as secure as it should be and recorded voices of children without parental consent in violation of the Children's Online Privacy Protection Act, 15 USC § 6501, *et seq.*, ("COPPA").[359] According to the complaint, consent was obtained by parents whose child owned the toy but the doll also captured the voices of other children whose parents had not provided consent.[360]

Around the same time, toymaker VTech Electronics North America was met with class action lawsuits filed by parents of children using VTech's electronic learning toys. VTech designs, manufactures and sells electronic learning toys for children that include software programs such as Kid Connect, which allows parents and children to interact with each other through online text messages.[361] VTech experienced a data breach in November 2015, compromising the personal information for millions of consumers, including children.[362] Shortly thereafter, consumers of VTech's products filed putative class actions in the U.S. District Court for the Northern District of Illinois.[363] According to the consolidated complaint, VTech (1) employed data security that was not as secure as it should have been, inconsistent with its

---

351 *Id.* at *2-3.

352 *Id.* at *3-4.

353 *Id.* at *35-36.

354 *Id.* at *35.

355 *Id.* at *12-13. On January 10, 2017, the judge lifted the stay on plaintiffs' remaining claims and set a new briefing schedule for the parties.

356 *See Archer-Hayes v. Toytalk, Inc.*, No. BC603467 (Cal. Super. Ct. filed Dec. 5, 2015).

357 *Id.* at ¶ 13.

358 *Id.* at ¶ 12.

359 *Id.* at ¶ 20.

360 *Id.* at ¶ 40.

361 *See Tittle v. VTech Electronics North America, LLC*, No. 1:15-cv-10889, at ¶¶ 10-11 (N.D. Ill. filed Dec. 3, 2015).

362 *Id.* at ¶ 2.

363 *See, e.g.*, *Giron v. VTech Electronics North America LLC*, No. 1:15-cv-11885 (N.D. Ill filed Dec. 31, 2015); *Tittle*, No. 1:15-cv-10889. In February 2016, a judge in the Northern District of Illinois consolidated five suits pending before him over VTech's toys. *See In re VTech Data Breach Litigation*, No. 1:15-cv-10889 (N.D. Ill. filed Feb. 24, 2016).

representations, and far below industry standards,[364] (2) was slow to detect the unauthorized access to its database,[365] and (3) responded inadequately when it learned of the data breach.[366] Plaintiffs' allege that VTech's "acts and omissions have placed Customers at serious risk of fraud and identity theft and, in the worst case, harm to young children . . . [and that] VTech Customers may have or will become victims of identity theft due to the breadth of the" November data breach.[367]

The lawsuit involving Hello Barbie was dismissed voluntarily with prejudice in July 2016 and litigation in the consolidated action against VTech has been stayed pending mediation. However, this looks like it will only be the start of litigation involving connected toys. Indeed, in December 2016, public interest organizations in the United States and the European Union submitted complaints to the FTC and EU Data Protection Authorities ("DPAs") describing various privacy and security weaknesses in connected toys produced by other manufacturers.[368]

Vulnerabilities in implantable medical devices also have started to attract attention. For example, in August 2016, a patient filed a proposed class action against St. Jude Medical in the U.S. District Court for the Central District of California.[369] The plaintiff alleged that St. Jude Medical failed to employ adequate security measures when remotely tracking its pacemakers and other heart-regulating implants.[370] According to the complaint, these medical devices are vulnerable to hackers:

> For example, by forging, altering, or replying to previously captured transmissions to or from an implanted cardiac device, a bad actor could monitor and modify the implant without necessary being close to the victim. Such attacks can put at risk the safety of the patient with the implantable device, with fatal consequences in certain cases.[371]

The plaintiff filed his complaint after a recent report by Muddy Waters Capital, which claimed to find security deficiencies in St. Jude Medical's remotely-controlled medical devices.[372] As with the lawsuits involving connected cars and toys, the plaintiff alleged that St. Jude Medical's devices were susceptible to a data breach but not that these devices had in fact been hacked. Just a few months after filing his complaint, the plaintiff voluntarily dismissed the litigation without prejudice.

---

364 *Id.* at ¶¶ 30-31.

365 *Id.* at ¶ 37.

366 *Id.* at ¶¶ 38-41.

367 *Id.* at ¶¶ 46, 48.

368 *See* Complaint and Request for Investigation, Injunction, and Other Relief, *In re Genesis Toys and Nuance Commc'ns* (FTC filed Dec. 6. 2016); *Connected toys violate European consumer law*, Forbrukerradet (Dec. 6, 2016), *available at* https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/. .

369 *See Ross v. St. Jude Medical Inc.*, No. 2:206-cv-06465 (C.D. Cal. filed Aug. 26, 2016).

370 *Id.* at ¶ 32.

371 *Id.* at ¶ 17.

372 *Id.* at ¶¶ 26 – 32; *see also* "St. Jude Medical, Inc.," Muddy Waters Capital LLC (August 25, 2016).

II. Insurance Coverage Issues Raised by the IoT

A. Cases Dealing with the Definition of "Property Damage"

Courts have long grappled with whether cyber-related losses are covered under first and third party insurance policies. In early cases, courts addressed coverage for losses to data or functionality of electronic devices that resulted from causes such as faulty equipment, power outages or malware. Today, courts all over the country continue to address these issues.

Generally speaking, policyholders have sought coverage for the loss of use of data or functionality of electronic devices on the ground that such losses involved property damage, which has been typically defined as including injury to or the loss of use of tangible property. In contrast, insurers have argued that such losses were not covered because those losses did not involve injury to or the loss of use of such property. Although courts have reached different conclusions on these issues, their reasoning may be instructive as courts begin to deal more specifically with coverage for tangible losses relating to IoT devices.

At one end of the spectrum is *American Guarantee and Liability Insurance v. Ingram Micro, Inc.*[373] The policyholder in that case, Ingram Micro, distributed "microcomputer products" and used a network ("Impulse") to track orders and keep information on its customers and products.[374] Due to a power outage, programming information that had been stored on Ingram Micro's mainframe computers was lost and had to be reprogrammed and Ingram Micro's data center was disconnected from the Impulse network for eight hours until a system switch was fixed.[375] Ingram Micro sought coverage for its resulting business and service interruption losses under an All Risks policy that Ingram Micro had procured from American Guarantee and Liability Insurance Company ("AGLIC").[376] This policy provided coverage for "'[a]ll Risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring . . . ."[377]

AGLIC argued that the All Risks policy did not cover Ingram Micro's business and service interruption losses because Ingram Micro's computer systems were not physically damaged, since the "power outage did not adversely affect the equipment's inherent ability to accept and process data and configuration settings when they were subsequently reentered into the computer system."[378] By contrast, Ingram Micro argued that the computer systems had been physically damaged because they had lost their functionality.[379]

The U.S. District Court for the District of Arizona sided with Ingram Micro, concluding that loss of programming information and customer configurations did constitute physical damage to tangible property. In so doing, the court explained:

> At a time when computer technology dominates our professional as well as personal lives, the Court must side with . . . [the] broader definition of "physical damage." The Court finds that "physical damage" is not restricted to the physical

373 No. 99-185, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000).
374 *Id.* at *2-3.
375 *Id.* at *3-5.
376 *Id.* at *3.
377 *Id.*
378 *Id.* at *5-6.
379 *Id.* at *6.

> destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.[380]

America Online, Inc. v. St. Paul Mercury Insurance Company represents the other end of the spectrum in these cases.[381] There, multiple class action suits had been filed against America Online ("AOL"), alleging that AOL's access software Version 5.0 caused plaintiffs' operating systems to crash and their computers to lose stored data. AOL tendered the defense of those suits to St. Paul Mercury Insurance Company, which had issued a commercial general liability (CGL) insurance policy to AOL.[382] The policy covered property damage, which was defined as:

> physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged.[383]

St. Paul denied AOL's claim on the ground that the underlying complaints did "not allege damage to 'tangible' property" under the CGL policy.[384]

In the resulting coverage litigation, the U.S. District Court for the Eastern District of Virginia, and then the Fourth Circuit Court of Appeals, agreed with St. Paul. In so doing, the Fourth Circuit analogized the loss of use of software on a computer to a lock combination and the lock itself, noting that "when the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval or resetting of the combination – the idea – the lock can be used again."[385] With this in mind, the court then explained that although AOL's CGL policy "cover[ed] any damage that may have been caused to circuits, switches, drives, and any other physical components of the computer," it did not cover "the loss of instructions to configure the switches or the loss of data stored magnetically." [386] Because "[t]hese instructions, data and information are abstract and intangible," the court held that damage to them "is not physical damage to tangible property."[387] Other courts have followed *American Online* and similarly concluded that damage to electronic data is not covered property damage.[388]

---

380 *Id. See also Centennial Ins. Co. v. Applied Health Care Systems*, 710 F.2d 1288, 1291 (7th Cir. 1983) (underlying complaint that alleged faulty controllers caused the loss of electronically stored data "clearly raise[d] the spectre that liability for property damage [might] ensue."); *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.3d 1264, 266 (N.M. Ct. App. 2002) (lower court had concluded data lost when policyholder reformatted a hard drive constituted tangible property, and the parties did not appeal that conclusion); *Retail Systems, Inc. v. CNA Ins. Companies*, 469 N.W.2d 735, 737 (Minn. Ct. App. 1991) (data on a computer tape was tangible constituted tangible property).

381 347 F.3d 89 (4th Cir. 2003).

382 *Id.* at 91-92.

383 *Id.* at 94.

384 *Id.*

385 *Id.* at 96.

386 *Id.*

387 *Id.*

388 *See e.g.*, *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 556 (Cal. Ct. App. 2003) (the loss of a computer database was not a direct physical loss or damage to covered property under the first party insurance policy at issue, as the court rejected the idea that "*information, qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch.").

B. Coverage for Damages Resulting from the Unauthorized Access to Data Under "Traditional" Liability Policies

Coverage disputes relating to data breaches may also be instructive as courts begin to deal with IoT-related coverage disputes. Policyholders seeking coverage for such breaches generally argue that their resulting losses constitute property damage under Coverage Part A of their general liability policies or advertising injury under Coverage Part B of those policies.

i. Data Breaches as Covered Property Damage

As a general matter, courts that have considered whether breach-related losses constitute "damage to tangible property," as required under CGL policies, have determined that they do not. For example, in 2012, the U.S. District Court for the Western District of Wisconsin addressed whether electronic funds in an on-line bank account were "tangible property" under a commercial excess liability and "Bis-Pak" policy.[389] In *Carlon*, the policyholder, Delaget, had been hired by a restaurant group to manage its finances.[390] The restaurant group's accounts were allegedly exposed to a virus on Delaget's computer and several hundred thousand dollars were stolen from the restaurant group's bank account.[391] Delaget argued that the term "tangible property" was reasonably susceptible to more than one meaning, and therefore, should be read to include electronic bank account funds.[392] The district court disagreed.[393] It concluded that the electronic funds at issue were not covered under the third party liability coverage form because there was no required loss of use of *tangible* property.[394]

More recently, a federal district court in Alabama reached a similar conclusion.[395] In that case, the policyholder, Camp's Grocery, was sued by three credit unions after a breach of its computer network.[396] In the underlying suit, the credit unions alleged that the data breach had compromised their customers' credit card, debit card and check card information.[397] Camp's Grocery sought coverage under a business owner's insurance policy, and when the insurer refused to provide coverage, Camp's Grocery filed suit.[398] Among other things, Camp's Grocery argued that the physical credit, debit, and check cards were "tangible property," and that the losses suffered by the credit unions in replacing these cards was "covered property damage."[399] Rejecting Camp's Grocery's argument, the U.S. District Court for the Northern District of Alabama concluded that the underlying claims were based on compromised *intangible* data contained on the cards that made the cards unusable.[400]

---

389 *See Carlon Co. v. DelaGet LLC*, No. 11-cv-477, 2012 U.S. Dist. LEXIS 70836 (W.D. Wis. May 21, 2012).

390 *Id.* at *3.

391 *Id.*

392 *Id.* at *14-15.

393 *Id.* at *14.

394 *Id.*

395 *See Camp's Grocery, Inc. v. State Farm Fire & Cas. Co.*, No. 4:16-cv-0204, 2016 U.S. Dist. LEXIS 147361 (N.D. Ala. Oct. 25, 2016).

396 *Id.* at *2.

397 *Id.*

398 *Id.* at *1.

399 *Id.* at *21.

400 *Id.*

ii. Data Breaches as Advertising Injury

The term "advertising injury" is typically defined in CGL policies as "a. Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services; b. oral or written publication of material that violates a person's right of privacy; c. misappropriation or advertising ideas or style of doing business; or d. infringement of copyright, title or slogan." Unlike the recent decisions considering whether breach-related losses constitute property damage, courts have reached different results when deciding whether such losses qualify as advertising injury.

In April 2011, Sony Corporation suffered a massive data breach in its PlayStation video game online network, which led to the theft of millions of customers' private information. Sony faced claims following a hack and it sought coverage under its general liability policies. In *Zurich American Insurance Company v. Sony Corporation*, a New York trial court was asked to decide whether the insurance companies were obligated to provide coverage for these claims.[401] In an oral opinion issued by Judge Oing, the court held that a "publication" took place when hackers breached Sony's network even though the hackers did not actually make the stolen information public.[402] However, pursuant to the general liability policies issued by Zurich, the "publication" had to be made by Sony itself.[403] Coverage could not be triggered by the actions of third parties.[404] Thus, Zurich's policies did not cover Sony's losses because the hackers rather than Sony were responsible for the "publication."[405]

On the other hand, in *Travelers Indemnity v. Portal Healthcare Solutions, L.L.C.*, the Fourth Circuit held that the insurer was obligated to defend its policyholder in a class action lawsuit alleging that the policyholder had made private medical records available on the Internet for several months.[406] In that case, confidential patient records kept by a medical records company were made available to unauthorized users.[407] The medical records company, Portal Healthcare, sought coverage under two commercial general liability policies for a class action lawsuit that had been filed against it.[408] The insurer argued that it was not obligated to provide coverage because Portal Healthcare's conduct did not effect a "publication" and no "publicity" occurred when Portal Healthcare posted the records online."[409] The district court disagreed, concluding that making the records publicly available on the Internet amounted to a "publication" that gave "unreasonable publicity" to and "disclose[d] information about patients' private lives" under the commercial general liability policies even though no third party was alleged to have viewed the information and Portal Healthcare took no steps to attract public attention to the information.[410]

On appeal, the Fourth Circuit affirmed the district court's decision, holding that the insurer had a duty to defend Portal Healthcare in the underlying class action because the alleged

401 No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014).
402 *Id.* at *70.
403 *Id.*
404 *Id.*
405 *Id.*
406 35 F. Supp. 3d 765 (E.D. Va. 2014).
407 *Id.* at 768.
408 *Id.*
409 *Id.* at 770-72.
410 *Id.*

conduct at least potentially constituted a publication of a the patients' confidential information.[411]

C. ISO Endorsements

In response to coverage disputes under traditional policies involving the loss of inability to access data and the unauthorized access to data, the Insurance Services Office ("ISO") has dealt with whether to exclude or limit coverage under tranditional policies for cyber-related losses. For example, after some courts had determined that electronic data could constitute tangible property, in 2001 the ISO issued a CGL coverage form which explicitly provided that electronic data was not tangible property.[412] In 2004, the ISO then introduced an exclusion (p) in the CGL form for "Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[413] But that same year, the ISO also introduced an endorsement through which policyholders could buy back limited coverage for "'property damage' because of all loss of 'electronic data' arising out of any one 'occurrence.'" That same endorsement defined the term "property damage" for purposes of the endorsement to include the "[l]oss of, loss of use of, damage to, corruption of, inability to access, or inability to properly manipulate 'electronic data', resulting from physical injury to tangible property. . . ."[414] Thus, this endorsement would apply where there has been a loss of or inability to access or manipulate electronic data only where there had otherwise been injury to tangible property.[415]

i. ISO Endorsement CG 24 13 04 13

More recently, through endorsements that went into effect in April 2013, the ISO amended the definition of "advertising injury" to which Coverage Part B applies. Recall that CGL policies typically define "advertising injury" as:

> a. Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services; b. oral or written publication of material that violates a person's right of privacy; c. misappropriation or advertising ideas or style of doing business; or d. infringement of copyright, title or slogan.

Endorsement CG 24 13 04 13 removes subpart (b) of that definition – and in so doing (inasmuch as policyholders have relied on subpart (b) in seeking coverage for data breaches), this

411 644 F. App'x 245, 247-48 (4th Cir. 2016).

412 ISO Policy Forms, Form Number CG 00 01 10 01. That amendment defined "electronic data" as "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

413 ISO Policy Forms, Form Number CG 00 01 12 04.

414 ISO Policy Forms, Form Number CG 04 37 12 04 at D.17.

415 ISO Policy Forms, Form Number CG 04 37 12 04. That same year, the ISO also introduced a claims made coverage for liability due to the loss of data, where computer hardware has not also been damaged. ISO Policy Forms, Form Number CG 00 65 12 04.

endorsement arguably defeats coverage in most cases for cyber liability claims as "personal or advertising injury."

ii. ISO Endorsement CG 21 06 05 14

Finally, the ISO endorsement CG 21 06 05 14, which went into effect in May 2014, impacts both Coverage Parts A and B by seeking further to limit recovery for cyber-related losses under traditional policies. With respect to Coverage Part A (bodily injury and property damage), the endorsement replaces exclusion (p) of CGL policies with the following:

> This insurance does not apply to: . . . [d]amages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including . . . any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

"Electronic data" means "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software . . . ." This endorsement also provides that the exclusion applies even if "damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by [the named insured] or others arising out of" that which is the subject of the exclusion.

Notably, there are two versions of this endorsement. Both versions have the language quoted above, but the second version also expressly excepts bodily injury from the exclusion by providing that "[u]nless Paragraph (1) above applies, this exclusion does not apply to damages because of 'bodily injury.'" This version of the endorsement thus indicates that damages due to bodily injury which arise out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data" may not be excluded from coverage, as long as the bodily injury did not arise from access to or disclosure of a person or organization's nonpublic information. This variation of endorsement CG 24 13 04 13 will likely be "front and center" in future coverage disputes, where policyholders are liable for bodily injury due to the hacking or other malfunctions of IoT devices.

Finally, with respect to Coverage Part B (personal and advertising injury), CG 21 06 05 14 also states:

> This insurance does not apply to: . . . "[p]ersonal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information . . . [t]his exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

An ISO executive explained the rationale for endorsement CG 21 06 05 14 at the time that it was introduced:

> At the time the ISO Commercial General Policies (CGL) were developed, certain hacking activities or data breaches were not prevalent and, therefore coverages related to the access to or disclosure of personal or confidential information and associated with such events were not necessarily contemplated under the policy.
> As the exposures to data breaches increased over time standalone policies started to become available in the marketplace to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information.[416]

Thus, the intent of the CG 21 06 05 14 seems to be to direct policyholders to standalone policies for coverage for cyber-related claims, with the notable exception of claims for bodily injury, where policyholders have purchased coverage with that version of the endorsement.

D. Coverage for Data Breaches Under Stand-Alone Cyber Policies

At the same time that courts have reached mixed results (at best) as to whether coverage is available for cyber-related incidents under traditional policies, and against the backdrop of the ISO's exclusionary endorsements, the market for stand-alone "cyber" policies has grown. Unlike traditional policies, which often have standard wording, there is no standard wording for cyber-related policies. Cyber policies typically present coverages for discrete types of cyber-related losses, such as first and third party losses arising from data breaches, network interruption, and extortion.

Although specialized policies have gained popularity in recent years, so far there have been few reported court decisions regarding the scope of coverage under these policies. Although the case law is thus less well developed, a few key cases underscore the importance of paying attention to policy terms and understanding the scope of coverage even when purchasing a specialized policy.

One of the first litigated disputes involving a stand-alone cyber insurance policy was *Columbia Casualty Company v. Cottage Health System*.[417] In that case, Cottage Health suffered a data breach that released private health care information on approximately 32,500 patients that was stored on its servers.[418] Columbia Casualty had issued a stand-alone NetProtect360 cyber insurance policy to Cottage Health and following the data breach, Columbia Casualty sought a declaration in the U.S. District Court for the Central District of California that it was not obligated to provide coverage for Cottage Health's losses.[419] More specifically, Columbia Casualty alleged that (1) the breach occurred because Cottage Health and/or its third party vendor stored the patient information on a system that was Internet-accessible and without the proper security measures, and (2) Cottage Health violated non-delegable duties under California law to maintain the security of confidential medical records and to detect and prevent data breaches on its systems.[420]

---

[416] "ISO Comments on CGL Endorsements for Data Breach Liability Exclusions," INS. J., July 18, 2014, *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm

[417] No. 2:15-cv-03432 (C.D. Cal. filed May 5, 2015).

[418] *Id.* at ¶ 16.

[419] *Id.* at ¶¶ 7-8.

[420] *Id.* at ¶¶ 17-18. Ultimately, this case was not decided on the merits. A few months later, the U.S. District Court Judge dismissed the suit to allow the parties to pursue alternative dispute resolution as provided for in the NetProtect360 cyber insurance policy.

Another early case was *Travelers Property Casualty Company of America v. Federal Recovery Services*.[421] Federal Recovery was in the business of processing, storing, transmitting and handling electronic data for other companies.[422] Federal Recovery entered into a Servicing Retail Installment Agreement with Global Fitness, pursuant to which Federal Recovery agreed to process member accounts and transfer member fees to Global Fitness.[423] A dispute erupted between the companies and Global Fitness sued Federal Recovery, alleging that Federal Recovery had retained possession of member data and interfered with Global Fitness' business dealings.[424] Federal Recovery tendered defense of the suit to Travelers, which had issued a CyberFirst Technology Errors and Omissions Liability Form Policy to Federal Recovery.[425]

Pursuant to the CyberFirst policy, Federal Recovery was entitled to coverage for losses caused by an "errors and omissions wrongful act," which was defined as "any error, omission or negligent act."[426] But in its complaint, Global Fitness alleged Federal Recovery "knowingly withheld [data from Global Fitness] and refused to turn it over until Global [Fitness] met certain demands.[427] Thus, "[i]nstead of alleging errors, omissions, or negligence, Global [Fitness] allege[d] knowledge, willfulness, and malice."[428] Accordingly, the U.S. District Court for the District of Utah concluded that Travelers did not have a duty to defend Federal Recovery in the Global Fitness suit.[429]

Additionally, just last year, in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, the U.S. District Court for the District of Arizona was asked to weigh in on the scope of coverage under a stand-alone cyber insurance policy. [430] P.F. Chang's, like many merchants, was unable to process credit card transactions itself.[431] As a result, it entered into an agreement with a third party, Bank of America Merchant Services (BAMS), to facilitate the processing of credit card transactions with the banks who issue credit cards.[432] Pursuant to the agreement, P.F. Chang's agreed to pay any fines, fees, or penalties imposed on BAMS by credit card associations, based on P.F. Chang's acts or omissions.[433]

In June 2014, P.F. Chang's learned that computer hackers had obtained about 60,000 credit card numbers belonging to P.F. Chang's customers and posted these numbers to the Internet.[434] After the cyber incident, credit card associations imposed on BAMS and, in accordance with their agreement, BAMS passed along the fees to P.F. Chang's.[435] P.F. Chang's then sought coverage for cyber-related losses from Federal Insurance under a Cybersecurity by Chubb Policy.[436] Federal Insurance reimbursed P.F. Chang's for $1.7 million in costs incurred by

421 103 F. Supp. 3d 1297 (D. Utah 2015).
422 *Id.* at 1298.
423 *Id.* at 1299.
424 *Id.* at 1300.
425 *Id.* at 1301.
426 *Id.* at 1302.
427 *Id.*
428 *Id.*
429 *Id.*
430 No. CV-15-01322, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016).
431 *Id.* at *3.
432 *Id.*
433 *Id.* at *4.
434 *Id.*
435 *Id.* at *6.
436 *Id.*

P.F. Chang's because of the data breach but it refused to reimburse P.F. Chang's for the fees assessed by BAMS.[437]

P.F. Chang's filed suit against Federal Insurance and Federal Insurance moved for summary judgment.[438] In support of its motion, Federal Insurance argued that the BAMS fees did not constitute a "Loss" as it was defined under the policy and, even if it did, coverage was eliminated by two exclusions which precluded coverage for liabilities assumed by P.F. Chang's without Federal Insurance's consent.[439] The Arizona federal district court agreed with Federal Insurance, concluding that the BAMS fees did not fall under the policy's definition of "Loss" and, in any event, these fees fell within the policy's exclusions concerning assumed liabilities.[440]

III. IoT Coverage Issues

To date, courts deciding coverage disputes following a data breach have considered whether the loss of electronic data constitutes property damage. However, with IoT products, a cyber-related loss could fall under the more traditional definition of covered property damage.

For example, the 2008 hack of a Polish train system discussed above resulted in a train derailment that injured at least 12 passengers and may very well have caused damage to the passengers' personal property and the property in the vicinity of the incident. In a situation like that one, the train company might, in the first instance, seek coverage for any third party claims under traditional general liability policies. If those general liability policies exclude coverage based on the unauthorized access of the train's electronic systems, there might well not be coverage. As discussed above, ISO endorsement CG 21 06 05 14 excludes "[d]amages arising out of: . . . (2) [t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." This would arguably exclude property damage (and, unless the adopted endorsement contains the limited exception, bodily injury) resulting from the hack if the train derailment were considered as damage "arising out of . . . [the] corruption of . . . electronic data." Having said this, policyholders like the train company might argue (especially as to policies that have not incorporated the more recent ISO endorsements, or that have adopted the variant of CG 21 06 05 14 which excepts bodily injury) that the focus should be on the resulting injury (not the cause), and that bodily injury and/or property damage emanating from the unauthorized access to data therefore should be covered.

The train company might also look to its cyber insurance policy for coverage. But unlike general liability policies, those policies tend to focus coverage for costs of more "typical" post-breach losses such as customer notification, credit monitoring, legal fees and fines. By contrast, those policies typically do not provide coverage for bodily injury or property damage.

Recently, however, certain carriers have started to offer insurance policies that include broader coverage for the types of losses that might occur after a cyber-incident. For example, some cyber insurance policies now cover bodily injury, property damage, business interruption and product liability related to a data breach. Even still, cyber policies offering coverage for a wider array of damages are not as commonplace right now; most cyber insurance policies do not provide such coverage. As a result, even if a company, like the train company, had purchased traditional insurance coverage and a stand-alone cyber insurance policy, that company might

437 *Id.* at *5-7.
438 *Id.* at *1.
439 *Id.* at *11-23.
440 *Id.* at *14-15, 24-25.

face complex insurance-related issues when property damage and/or bodily injury occurs after a cyber-attack, as in the example just discussed.

Beyond coverage for bodily injury and property damage, the interconnectedness of a widespread number of devices presents other issues. Information stored on one IoT device is only as protected as the least secure device connected to the same network. Regardless of how secure a particular device is on its own, if it is connected to a network, the security of that device could be vulnerable due to lack of security of a completely different device connected to that network. This has the potential to compromise a policyholder's ability to seek coverage under it stand-alone cyber policy.

As mentioned above, in the case of *Columbia Casualty Company v. Cottage Health System*, Columbia Casualty sought a declaration that it was not obligated to provide coverage for its policyholder, Cottage Health, under a NetProtect360 cyber insurance policy after a data breach released tens of thousands of patient medical records stored electronically on Cottage Health's servers.[441] Columbia Casualty alleged, in part, that the cyber incident occurred because Cottage Health and/or its third party vendor had stored the patient files on a system that lacked the proper security measures contrary to the representations Cottage Health made on its insurance application.[442]

Such representations are commonly required in cyber insurance policy applications. Where the security of one connected device depends on all other devices connected to the same network (potentially including devices outside of the policyholder's control), this could complicate a policyholder's ability to make representations regarding the security measures in place and/or comply with a cyber insurance policy requirement to maintain certain security measures.

IV. Conclusion

The explosion of the IoT brings many opportunities. However, it also comes with a wealth of unique risks. Controlled demonstrations and actual cyber incidents have shown IoT products to be susceptible to attacks. The next wave of insurance coverage litigation may very well involve these products as manufacturers derive new and creative ways to connect everyday objects to the Internet. As losses that are more disastrous occur with the mainstream use of these products, courts will be faced with complicated insurance coverage questions regarding the interplay between various insurance policies. As a result, it will be all the more important for insurance carriers and policyholders to pay careful attention to the specific terms of their insurance policies to make sure that the available coverage satisfies both parties' expectations.

441 No. 2:15-cv-03432.

442 *Id.* at ¶¶ 17-18.

About the Authors

Ellen M. Farrell is a senior counsel in Crowell & Moring's Insurance/Reinsurance Group.

Rachel P. Raphael is an associate in Crowell & Moring's Insurance/Reinsurance Group.

Discussion Questions

1. Should there be one, single federal agency with oversight of the IoT, instead of multiple different agencies, each dealing with one specific sector?

2. How could traditional property and casualty insurance policies be reconciled with the "intangible" nature of IoT?

3. Would cybersecurity coverage policies vary among economic sectors and subsectors, due to their different characteristics, requirements, and needs?

To Cite this Article

Farrell, E. M., & Raphael, R. P. (2018, Fall). The Internet of Things: Insurance coverage considerations. *Journal of Multidisciplinary Research, 10*(3), 61-80.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 81-104.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

The Internet of Things: A Mosaic

H. Michael O'Brien
Wilson Elser

Abstract

This article begins with Part 1, a piece about security concerns with IoT connectivity, impact on product liability, and possible consequences. Parts 2 and 3 focus on product liability in the automotive industry, Part 4 on Government oversight, and Part 5 on security and the industrial Internet consortium. The author then addresses the issue of cyber vulnerability, expanding coverage to risks of physical threats; next, he states the new landscape of IoT would require the formation of a new breed of experts and lawyers; finally, he concludes on regulatory issues and the guidelines of the Consumer Product Safety Commission.

Keywords: Internet of things, connectivity, product liability, consortium, vulnerability, regulation

Introduction

Michael O'Brien has covered a broad spectrum of IoT issues with blogs posted on the website of Wilson Elser, of which he is partner in the New York office. This article is a composite mosaic of blogs by O'Brien from 2015 until today. This article begins with a series of blogs in five parts, opening with a February 2015 Part 1 piece about security concerns with IoT connectivity, impact on product liability, and possible consequences. In July 2015 followed Parts 2 and 3, focusing on product liability in the automotive industry. In October 2015 followed Part 4 on Government oversight; in November 2015, the series closed with Part 5 on security and the industrial Internet consortium. O'Brien followed up with four stand-alone pieces: In March 2016, the blog addressed the issue of cyber vulnerability, expanding coverage to risks of physical threats in June 2017. In December 2017, O'Brien submitted that the new landscape of IoT would require the formation of a new breed of experts and lawyers, and in April 2018, he concluded the series on regulatory issues and the guidelines of the Consumer Product Safety Commission. The Guest Editor would like to thank Mr. O'Brien and Wilson Elser for permission to adapt and reproduce these blog posts in this article.

The Internet of Things: The Inevitable Collision with Product Liability
Part 1 (February 2, 2015)

With IoT connectivity, the potential for energy savings derives from using IoT products during off-peak energy periods. This application already exists in many central heating and air–conditioning applications. Other opportunities for the programmable use of appliances include washers, dryers and dishwashers in off-peak time.

The second benefit is in the area of tech services, performing a diagnostic from a remote location and either correcting the problem remotely or dispatching the service tech who will know what the problem is in advance.

Security Concerns

The proliferation of applications for IoT devices is raising concerns with respect to the security of these devices and the purposes for which personal data collected will be used. The use of IoT technology therefore introduces a new layer of risk for these products, which raises concerns about privacy and the potential for outside interference by individuals or groups with nefarious motives.

Could the vulnerability of IoT devices and products actually encourage such attacks against consumers? The answer is probably yes. A study released by Hewlett-Packard in 2014 found 70 percent of IoT devices are vulnerable to attack. The vulnerabilities identified in the report include password security, encryption and general lack of granular user access.

In 2014, the German government's federal office for information security (the BSI) released details of an attack on the network of a steel plant. The perpetrators eventually gained access to the plant's production network and other systems and took control of a blast furnace, preventing it from shutting down, which caused massive damage to the system. This was identified as the second cyber-attack to cause physical damage; the first known attack was the Stuxnet malware attack on the Natanz uranium enrichment plant in Iran.

In the consumer setting, the FTC report provides some examples of potential vulnerabilities:

Smart televisions that store or transmit information could be exploited to compromise personal information.

IoT devices may be used to facilitate attacks on the consumer's network or on other systems, including denial-of-service attacks.

The risk to physical safety was also noted. One member of the FTC group studying the problems stated he was able to hack two insulin pumps from a remote location and changed the settings to deny delivery of medicine.

Another example was the hacking of a car's computer system from a remote location.

The FTC report notes that the proliferation of inexpensive IoT devices may be part of the risk to consumers. IoT device makers may not be attuned to the security issues and lack the economic incentives to provide software updates and support when vulnerabilities are discovered.

In the private sector, similar concerns are being voiced. Michael Coates, director of product safety at Sharpe Security and chairman of OWASP (Open Web Application Security Project), has predicted that the lack of updates to IoT consumer devices will become an area of vulnerability for manufacturers because it will "be a very low priority for the manufacturer."

Coates also predicts "criminal organizations will run their malicious activities in the background without impacting the overall performance of the device and this will mean the customer will not notice the malware, and the security vulnerability will have no impact on the performance of the device. These kinds of vulnerabilities could result in the loss of private data that will be monitored and sold without their knowledge."

Coates, like the FTC, forecasts effective patches as a problem: "Once it is discovered, the manufacturer will rush to issue a patch. But, how will the patch be delivered? Will consumers have to reboot their oven? Will the updated software only be available in the next release of the physical product?"

The Impact on Product Liability

There are at least three areas of vulnerability for consumers and businesses that are fairly predictable:

First is the simple malfunction of an IoT product due to a software glitch that could result in physical damage to property or personal injury. For example, an IoT furnace control could fail during cold weather in an unoccupied home leading to frozen pipes and water damage.

Second is an attack from an outside source. For example, a gas range in a home could be subject to a cyber-attack causing fire and property damage.

Third, an IoT product or server is hacked and personal data is downloaded and used by the hacker. Imagine the personal data stored on your television and computer stolen and used in a denial of services attack.

These types of problems, if widespread within a product line found to be vulnerable to such malfunctions and attacks, could lead to product liability law suits and class action litigation by the affected consumers.

Liability and Consequences

In each of these hypothetical situations, one can ask: "Who will play a role in the allocation of fault and who will bear the financial consequences?"

Under the traditional principles of strict liability, fault flows up the chain of distribution from the retailer through mid-channel distributors ultimately to the manufacturer. But will the software developer for an IoT product or handheld device be brought into the equation when an IoT product causes a loss? Who will bear the responsibility if the software is vulnerable to an outside attack? These risks are often addressed between parts suppliers and manufacturers under the terms of supply agreements where a contractual duty to defend and indemnify against damages caused by a malfunctioning device is spelled out.

What role will the consumer play? Will the consumer become a target for fault apportionment if it is found that the consumer failed to update security software or used easily hacked passwords or downloaded malware from unsecure sites? What issues of privacy will develop when litigation is brought and demands are made by potentially liable third parties to examine the device used by the consumer and download its contents? What issues of privacy will arise when information downloaded from an IoT product is stolen? What issues of privacy will exist when information collected from an IoT-connected device is sold by the IoT device manufacturer to a third party?

How will the losses be investigated and will responsibility for failure of an IoT product prove more difficult to investigate and thus to establish liability? What types of experts will now be called on to play a role in the investigation?

The Internet of Things and the Inevitable Collision with Products Liability Part 2: One Step Closer (July 15, 2015)

The Internet of Things and the Inevitable Collision with Products Liability, published in February 2015, identified a number of factors leading to the emergence and phenomenal growth of the Internet of Things (IoT). It also identified issues relating to potential product liability exposures and the impact that IoT-connected devices could have on risk assessment and risk transfer due to the consequences of foreseeable vulnerabilities and failures with IoT-connected products.

This second article addresses in more detail the emerging liability risks for the stakeholders at the forefront of the development and implementation of these technologies who, in turn, will be forced to confront those liabilities whether or not they are prepared to do so.

Several documented IoT failures have already occurred in 2015. Notably, Wink's wireless hub, which is connected to a variety of devices in homes via a single app, experienced a failure in April that disabled the connected devices, potentially leaving consumers vulnerable to breach of their home security systems or other failures. Chamberlain and Ooma also experienced failures, both of which involved compromised IoT connective services and resulted in disruptions that had the potential to affect customers' home security.

The first IoT class action was brought in March 2015 spurred by the February publication of a report by U.S. Senator Edward Markey (D-MA), which was also covered on a CBS broadcast of 60 Minutes. The action was brought against Toyota Motor Corporation, Ford Motor Company and General Motors LLC. (See Cahen, et al. v. Toyota Motor Corporation, et al., U.S. District Court of Northern California, San Francisco Division, Civil Action No. 4:2015cv01104.)

Senator Markey's staff questioned 16 auto manufacturers regarding how they protect against vulnerabilities of vehicles to the threat posed by outside hackers infiltrating vehicle systems that could lead to loss of control over vehicles or disabling of safety devices. (See Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk.)

The investigation was prompted by studies that disclosed that hackers can get into the controls of some popular vehicles, causing sudden acceleration, turns, loss of brakes, activation of the horn, faulty operation of the headlights, and modification of the speedometer and gas gauge readings.

Senator Markey's investigation was therefore directed at determining what automobile manufacturers are doing to address these issues and protect drivers.

According to the report, based on the auto manufacturers' responses, a number of serious vulnerabilities were identified:

Nearly 100 percent of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.

Most automobile manufacturers were unaware of or unable to report on past hacking incidents.

Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers.

Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real time, and most say they rely on technologies that cannot be used for this purpose at all.

Additional concerns about driver privacy were identified as navigation systems and other features can record and send location or driving history information. This topic will be explored in greater detail in a future segment of this series.

The complaint filed in the resulting class action brought against the auto manufacturers closely mirrors the threats identified in the Markey report. The core allegations made against each auto manufacturer are based on breach of warranty claims that the vehicles are not free of defects: "Because defendants failed to ensure basic electronic security of their vehicles; anyone can hack into them, take control of the basic functions of the vehicle, and thereby endanger the safety of the driver and others."

The complaint further alleges that each vehicle has up to 35 separate electronic control units (ECUs) that interact with controlled area networks (CANs) and "vehicle functionality and safety depend on the functions of these small computers, the most essential of which is how they communicate with one another." As a result, a "hacker could take control of such basic functions of the vehicle as braking, steering and acceleration – and the driver of the vehicle would not be able to regain control."

This action is still in its early procedural stage, so forecasting the merits and outcome is premature, but nonetheless it should provide cause for concern for manufacturers and software companies that are actively developing products for the IoT marketplace.

Other Threats Identified

In April 2015, the U.S. Government Accountability Office (GAO) issued a report addressing commercial aircraft safety from cyber threats. GAO noted that "modern aircraft are increasingly connected to the internet, [but this] interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems." (See Air Traffic Control – FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen.)

Among GAO's conclusions, the report found "…FAA has taken steps to protect its ATC (Air Traffic Control) systems from cyber based threats; however significant security control weaknesses remain to ensure the safe and uninterrupted operation of the national airspace system."

The FBI is reported to be investigating an individual who claimed through social media that he had hacked into passenger airplane controls while on board flights and had taken over command of certain airplane functions. The intrusion was reportedly made through Wi-Fi access via the plane entertainment system. (See The Washington Post, May 18, 2015.)

Swiss Re in May 2015 published a global risk assessment report in which it identified the Internet of Things as among the highest potential risk impact comparable only to de-globalization, the great monetary experiment and supernatural category storms. (See Swiss Re SONAR, New Emerging Risk Insights.)

More recently, AIG has published part one of a series of white papers addressing IoT risks, The Internet of Things: Evolution or Revolution. The report predicts significant risks for businesses entering the global market for IoT-connected products:

"From cyber breaches to shifting questions of property and products liability, businesses cannot afford to enter this new technological world unprepared. For example, every object that

connects with the Internet is another entry point through which the cyber-criminals can enter a business' [sic] enterprise system. Equally dangerous, in a world where machines replace humans as the decision-makers and sensors are continually capturing data, serious questions of liability, resulting physical damage and privacy arise."

As to liability concerns, the paper posits a number of thought-provoking scenarios:

"When it comes to autonomous vehicles, like driverless cars, we are faced with an obvious ethical dilemma: In the seconds before an accident, should an autonomous vehicle do anything it can to protect the passengers, even if it means harming other motorists or pedestrians? When humans are behind the wheel, collateral damage, as terrible as it is, doesn't pose much of an ethical problem. A human being in danger can't be faulted when its survival instincts make it swerve its car into a pedestrian. But when machines are the decision-makers, does a pedestrian harmed in accident have a case against the car manufacturer? Does a driver have a case against a car manufacturer following an accident in which he or she was injured?

"IoT devices also raise troubling questions when it comes to device malfunction. Sensors can be embedded in critical infrastructure like dams, bridges, and roadways to monitor structural integrity as well as environmental conditions that could undermine structural integrity. A road near a flood area could be embedded with sensors that know the moment rainfall has exceeded a point that gives engineers advanced warning of flooding. Indeed, protecting infrastructure is one of the most exciting aspects of IoT. Yet when we turn more and more of our critical infrastructure and security systems over to IoT objects, we run the risk of a catastrophe if and when those objects fail. We can apply this to the private sector as well. To cite a non-lethal example, in April 2015 several American Airlines flights were delayed when a software malfunction rendered pilots' tablets, which they use for navigational purposes, useless. Although the malfunction was easily fixed with a software update, these examples show just how exposed we already are because of our connected devices. When—not if-– they fail, will we be prepared?"

Supply Chain Considerations

Software vendors and sensor manufacturers are now critical component part suppliers in the development of IoT-connected products. Major players in the development of IoT products and applications are acquiring software companies and partnering with Internet start-ups to take strategic advantage of the emerging market. Google, Microsoft, Samsung and Amazon have all made recent acquisitions of companies that will accelerate their penetration of the multibillion-dollar IoT marketplace. Strategic joint venturing between technology companies and other business enterprises seeking to catch the wave are also occurring weekly. These new strategic partnering initiatives will have an impact on component part suppliers' product liability exposures, most notably the software vendors and sensor manufacturers.

Component parts manufacturers have long been subject to product liability exposures when a critical component part causes or fails to prevent a product failure.

Sensor manufacturers will face greater liability exposure in part simply because of the greater use of sensors in all manner of IoT product applications. Sensors have already been the subject of product liability claims and lawsuits for alleged failures in products such as smoke detectors, carbon monoxide alarms and automobile airbag systems.

In the IoT world, software licensors will not be protected against third-party injury claims. Many software vendors have either (1) been unaware of their product liability exposure

to claims and lawsuits for bodily injury and property damage caused to third parties or (2) have failed to provide for such exposures in their agreements. Licensing agreements and their built-in provisions for protection against failures have largely been limited to instances of failures or damages between a software vendor and its customer, and specifically related to the task for which the software was provided. These agreements may not insulate a software vendor from liability resulting from a failure that injures a third party or causes property damage to a third party for which such loss was foreseeable.

Insurance coverage for losses that result in property damage or bodily injury is an area of vulnerability for stakeholders. Traditional cyber-data breach insurance coverage addresses the loss in intangible property as a result of a breach. An IoT product failure that results in property damage or bodily injury will, in the absence of a specifically designed policy, require companies to look to the traditional coverage afforded under CGL, PL, D&O and E&O policies. Inevitably, in the absence of specifically designed coverage there will be instances where gaps will exist and the exposure will be uninsured.

Software companies and product manufacturers need to and will develop contractual language to properly balance and shift the potential third-party liability exposures. However, the enormous financial power differentiations between the big technology players and the medium-sized to small software start-ups and new IoT-centric businesses will require that adequate financial protections in the form of IoT insurance coverage be developed. The insurance industry to date has been slow to recognize the enormous potential market for IoT insurance coverage for commercial liability exposures. It has been predicted that companies such as Google, Amazon and Apple with their huge liquidity may jump in and take a leading role at the expense of insurers. This development has already begun to unfold in personal lines insurance where technology companies have a huge advantage over insurers with the collection and use of data from consumers. Insurers are also coming around to recognize the power of big data and have initiated their own strategic partnering with technology companies such as American Family Insurance Company and Microsoft's joint enterprise to create an accelerator for startups focused on smart home technology.

Lack of Standards

One of the immediate short-term concerns for stakeholders is the lack of uniform standards for the IoT whether it is industrial IoT, consumer goods or other applications. The lack of uniform standards will result in vulnerabilities for IoT companies when the inevitable accidents occur leading to claims and lawsuits. Plaintiff attorneys will be certain to seize on the lack of self-governance within the industry based on the lack of recognized minimum standards for safety and security.

Currently, standards-setting organizations are working on developing standards that will be implemented at some point in the future. These include:

Institute of Electrical and Electronics Engineers (IEEE): P2413 Draft Standard for an Architectural Framework for The Internet of Things Working Group

International Telecommunications Union (ITU): Y2060 – Overview of The Internet of Things.

Industry security specialists have sounded the alarm over concerns with the fast-paced development of IoT without adequate security safeguards. A June 14, 2015, interview of two security specialists that appeared in *The Globe and Mail* noted:

> The key weakness of most tech companies and their Internet of Things (IoT) customers is a failure to create a 'threat model' and test security against that. If they don't know what they are trying to defend, and who they are trying to defend it against, any security measure and no security measure applies. You attack the weakest device, and an IoT device usually has weak or no authentication with other devices in the same network.
>
> Another security specialist noted in a Pace interview:
>
> Despite the industry's best efforts, the IoT will never be 100% secure … We don't know all of the ways that smart devices will interact with each other and how they will be used. The complexity and scale of the IoT will inevitably lead to security holes. A detect-and-respond mindset must be adopted from the start. … Manufacturers and other businesses should assume that the IoT technology stack will be attacked, and be properly prepared to respond. This means investing in systems that automate the detection of malicious activity so that it can be contained and remediated before data is lost or damage is done.
>
> Users can't be expected to download antivirus software for every smart connected device – it may not even be possible given the disparity of operating systems. At the same time, businesses can't be expected to deploy patches and updates to disposable, lightweight devices. IoT devices must be built with security and privacy controls baked in. Networks must be instrumented to automatically detect malicious behaviour.

Next up in Part 3. The IoT and privacy as it relates to data collection from IoT devices. Who owns the data? Who is responsible for its security? What steps are necessary to inform and protect consumers' data from unauthorized uses or hacking threats? Also, what will be the reporting obligations for IoT product defects to government safety agencies? Who will be obligated to report? What event may trigger an obligation to report when there is a threat of physical damage or bodily injury arising from an IoT device defect?

The Internet of Things and the Inevitable Collision with Products Liability
Part 3: Initial Contact (July 28, 2015)

This is the third in a series of blogs examining the rapid development of the Internet of Things (IoT) and its consequential impact on product liability risk. The development of the IoT has been so rapid and the applications so ubiquitous across every imaginable industry and commercial enterprise that there has been a failure by many businesses to recognize that with interconnectivity of so many products and services, security is only as strong as the weakest link within the chain of interconnected products.

This structural weakness became all too evident when Fiat Chrysler announced on July 24, 2015, the recall of 1.4 million vehicles due to a cyber security flaw disclosed by technology journal Wired. Hackers were able to remotely commandeer a Jeep's controls through the vehicle's Internet communications systems. (See "Hackers Remotely Kill a Jeep on the Highway – With Me in It," Wired, July 2015.) Along those same lines, the vulnerability of most current-model automobiles was identified and publicized recently by two separate government investigations. (See FTC report and Senator Markey's report.)

The National Highway Traffic Safety Administration (NHTSA) has commenced an investigation and Fiat Chrysler is working with NHTSA to facilitate this investigation. According to press reports, an open communications port within the Wi-Fi radio system is the weak link. Fiat Chrysler reportedly first identified the flaw in January 2014, but did not know at the time that it could affect critical vehicle controls. The announced fix is a software patch that will be installed by a USB device sent to owners of the affected vehicles.

This recent recall underscores the potentially enormous vulnerabilities IoT products have to hacking if security is not made an absolute top priority. Software failures that lead to a malfunction of a product resulting in physical damage or injury highlight but one predictable vulnerability in mass-produced products. The threat of a deliberate exploitation of a software defect by a malicious third party is an entirely new category of risk the dimensions of which product manufacturers and software companies are only now beginning to recognize. (See "Five Lessons on the 'Security of Things' From the Jeep Cherokee Attack," Forbes Tech July 27, 2015.)

The Fiat Chrysler recall illustrates the importance of adequate cyber security as a necessity from the ground up and provides a preview of how manufacturers and software companies will be required to address these flaws, which can affect millions of products. It also highlights the role of closely working with the appropriate federal safety agency in order to get out ahead of a potential crisis before it results in property damage or injury.

Some Takeaway Considerations

Some articles suggest Fiat Chrysler is working with the software vendor to correct the problem. If so, it may present a liability exposure to the software vendor depending on, among other things, what is contained in the contract between Fiat Chrysler and its software vendor for defects in the software.

Product liability recall insurance can be expensive. If the software vendor is on the hook to absorb part or all of the recall expenses, those expenses may come directly out of its own pocket.

In the immediate aftermath of the publication of the vulnerabilities of motor vehicles to Internet hacking, U.S. Senators Edward Markey of Massachusetts and Richard Blumenthal of Connecticut introduced legislation that would empower NHSTA and the Federal Trade Commission to establish rules to secure vehicles from hacking threats and maintain driver privacy. (See Spy Car Act of 2015.)

The Internet of Things and the Inevitable Collision with Product Liability
Part 4: Government Oversight (October 16, 2015)

The exponential growth of the Internet of Things (IoT) is far outpacing the ability of stakeholders to address safety standards and security concerns. This is not unusual as rapidly developing technology often challenges regulators and standards organizations to develop a framework for consensus governance. However, because the IoT transcends so many industries, there will be unprecedented difficulties with respect to harmonization of standards that will apply from one industry sector to another.

The efforts to develop and implement safety standards and government regulations have been taking place globally, albeit in fits and starts and not necessarily in synchronization among

the developed countries. Nonetheless, as governments take note of the IoT, the number of threats identified continues to multiply.

Red Flags for Datamining

On September 10, 2015, the Federal Bureau of Investigation (FBI) posted online a public service announcement warning of IoT risks for cybercrime, which include vulnerabilities to individuals' and businesses' personal data as well as the potential for "compromising the IoT device to cause physical harm." [Emphasis added.] Universal Plug and Play (UPnP) protocol used to access many IoT devices was identified as being especially vulnerable to exploitation.

AT&T reported in its Cybersecurity Insights, Volume 1, October 1, 2015, that it had seen a dramatic 458 percent increase in IoT vulnerability scans against IoT-connected devices.

Business and technology writer George V. Hulme wrote recently "… security is no longer just about data and access to IT systems and applications. It's also about how all those linked physical devices communicate, and that adds a new and dangerous dimension. With everything interconnected, everything is also now at risk of Internet-based attacks that look just like cyberattacks we see today, with data theft, denial-of-service exploits and malicious hackers hijacking devices and making them do their bidding – only on a potentially much larger scale." He goes on to cite the international research and analysis group IDC as reporting that it "… expects 90 percent of networks will have an IoT breach within two years."

The Wall Street Journal reported on August 6, 2015, about Yodlee, a business that among other things buys and sells data. Yodlee provides online personal finance tools to a number of the largest U.S. banks. When the banks' customers use the tools supplied by Yodlee, it sells some of the data to other businesses, such as hedge funds, that use the data for predictive analytics. The article characterized the information collected and sold as "more granular than ever," allowing investors to look into specific transactions by consumers in advance of securities filings to gain an advantage in estimating revenue. The article noted that while steps are taken to scrub the data Yodlee sells to its customers to protect privacy and that it requires that buyers not re-sell the data, researchers at MIT claimed they can unmask roughly 90 percent of people in a data base of anonymous credit card transactions with as little as four pieces of information.

Mining personal data is, in fact, nothing new. Security expert and author Marc Goodman in his recently published book Future Crimes describes many instances where personal data of individuals is collected and sold to third parties. Google and Facebook are identified among the major players. Goodman characterizes consumers who freely give up their personal data as a result of accepting the conditions contained in the Terms of Service (ToS) agreements with Internet companies, in effect becoming the "product" not the actual customer. The real customer is in fact the companies buying the data from the Internet companies. Thus, the exponential growth of IoT will undoubtedly fuel the efforts by companies to collect and harvest data from all manner of interconnected products and create new markets for the acquisition of personal data.

Report to the President

In November 2014, the National Security Telecommunications Advisory Committee (NSTAC) issued its Report to the President on the Internet of Things. The committee noted: "In 2008, the U.S. National Intelligence Council warned that the IoT would be a disruptive technology by 2025 … [Seven] years later, this warning remains valid, though it now seems

certain that the IoT will be disruptive far sooner than 2025 – if it is not so already." [Emphasis added.]

Among the more compelling and thought-provoking findings reached by the committee were:

"The line between consumer and industrial devices continues to blur, with consumer devices used – intentionally or not – in ways that affect national security/emergency preparedness (NS/EP). The strong growth in interconnected, potentially adaptive devices implies a larger cybersecurity attack surface with potentially cascading adverse effects in both the cyber and physical domains."

"IoT represents a convergence, or perhaps a collision, of IT [information technology] and OT [operational technology]. To this point, the two disciplines have approached cybersecurity differently. IT security involves patches and frequent updates and the ability to take systems offline as needed, while OT security is largely based on obscurity and specialization, in large part because of the need for systems to remain online, whether compromised or not. This disconnect creates gaps that attackers could exploit."

"Innovation and adoption of IoT technology are outpacing the development of IoT governance structures and related policies. This appears to be true at both the national and global levels."

"The emergence of IoT and the convergence of IT and OT demand experts who understand and can respond effectively to these new challenges. Academic programs that integrate core concepts and the implications of new interdependencies are needed, as are training programs for practicing professionals in both IT and OT and in the development of future IoT."

Since the report was issued, Congress has stepped up its efforts to investigate the IoT and its implications for good and ill.

In February 2015, the U.S. Senate Committee on Commerce, Science and Transportation held a hearing titled "The Connected World: Examining the Internet of Things."

In March 2015, the U.S. House of Representatives Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade held a hearing on the Internet of Things.

In March 2015, the U.S. Senate passed a resolution aimed at tackling many of these concerns.

On June 23, 2015, a group of U.S. senators sent a letter to the Government Accountability Office (GAO) to undertake a study to determine among other things the technical standards needed for various devices to efficiently communicate with each other and with users.

On July 29, 2015, the U.S. House of Representatives, Subcommittee on Courts, Intellectual Property, and the Internet held a hearing on the current and future challenges facing the Internet of Things.

Government Action versus Self-Regulation

In response to these developments, industry leaders have expressed concerns to Congress that such efforts at regulation could stifle innovation. In addition to hearings, federal agencies are taking action to make businesses implement measures to ensure cybersecurity is at the foundation of the development of any product that will connect to the Internet.

In March 2015, the Federal Trade Commission (FTC) established the Office of Technology Research and Investigation (OTRI) as the successor to the Mobile Technology Unit (MTU). The OTRI "… will build upon the groundwork by tracking an even broader array of investigative research on technology issues involving all facets of the FTC's consumer protection

mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data and the Internet of Things."

In addition, the FTC published a primer for IoT businesses that provides some basic guiding principles for IoT device manufacturers and software companies to take into account in order to build a platform of security from the ground up. The FTC notes that "[w]hat's reasonable will depend on a number of variables, including the kind and amount of information collected, the type of functionality involved, and the potential security risks."

Meanwhile, in January 2015, The Online Trust Alliance (OTA) created the IoT Trustworthy Working Group (ITWG), a multi-stakeholder initiative, that in August 2015 issued an IoT Trust Framework discussion draft for the Internet of Things. The framework focuses on best practices in security and privacy and sustainability within two primary categories: (1) home automation and connected home products and (2) wearable technologies, limited to the health and fitness categories.

The End Game

Sustainability has been identified as a critical area for security – a device that is secure when bought could eventually become vulnerable if not properly supported. This entails recognizing that security and privacy must by design be a priority from the outset of product development and be addressed holistically focusing on end-to-end security and privacy.

The ITWG's IoT Trust Framework proposes 23 minimum requirements and a commitment to comply with all relevant regulatory requirements. In addition, there are 12 other recommendations that go above and beyond the initial recommendations.

Among the areas requiring minimum compliance are making the privacy policy readily available, optimizing the design for user interface, identifying all personally identifiable data collected, providing data purging options for users and incorporating encryption by default.

These fledgling efforts by industry, government and technology advocacy groups are going to be challenged to keep pace with the speed at which IoT applications are multiplying. New stakeholders, including experts from all walks of science, industry, business, insurance and the legal profession, will need to join forces proactively sooner rather than later to help the IoT fulfill its promise and hopefully minimize the real and potential threats involving physical damage, personal injury, or compromised personal data and security.

The Internet of Things and the Inevitable Collision with Product Liability
Part 5: Security and the Industrial Internet Consortium (November 24, 2015)

The rapid emergence of the Internet of Things (IoT) led to the establishment of the Industrial Internet Consortium (IIC) in the spring of 2014 by five primary stakeholders: AT&T, Cisco, General Electric, IBM and Intel. IIC now claims a membership of 211 in more than 26 countries. Each of the five founding members, like many other companies, is undergoing significant transformations within their core business platforms to take advantage of the immense growth opportunities with IoT.

On November 3, 2015, the IIC held its initial Industrial Internet Security Forum at IBM's New York City headquarters. Not surprisingly, security, security and more security was the theme du jour.

Part of IIC's mission statement is "To bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices." Its goals are to:

Drive innovation through the creation of new industry-use cases and test beds for real-world applications

Define and develop the reference architecture and frameworks necessary for interoperability

Influence the global development standards process for Internet and industrial systems

Facilitate open forums to share and exchange real-world ideas, practices, lessons and insights

Build confidence around new and innovative approaches to security.

Guest speakers at the program were members of the IIC and security experts. Key takeaway points from this meeting include the convergence and friction between information technology (IT) and operational technology (OT); the inevitable identification of payloads for IoT cyberattacks; interoperability issues and defense of legacy technologies; and perimeter defense and partition of systems to improve security. All of these terms and concepts were addressed by speakers and panelists to define IoT security within the Industrial Internet.

Opening remarks by Lynne Canavan, IIC's Vice President of Program Management, emphasized IIC's mission statement and the charter of the Security Working Group to "define a security and privacy framework to be applied to technology adopted by the IIC." This "will establish best practices to be used to identify security gaps in existing technologies."

Key Drivers

Brian Dalgetty of IBM IoT, Industry Solutions, identified some of the key driving and disruptive forces of IoT, which include improving operations and lowering costs, creating new business models and products, and driving engagement and customer services. Among the challenges identified were (1) the unprecedented data volumes, (2) fundamental shifts in business models, (3) incompatible standards, (4) entirely new security threats and (5) the new privacy landscape.

While big data is one of the driving forces behind the IoT, Dalgetty observed that 60 percent of data collected loses its value within seconds. Part of IBM's strategy is to partner with companies that provide services for the IoT, and not necessarily to make new things. IBM wants to capture data and use it to transform businesses. To that end, it is developing horizontal platforms with partners. Collecting and capturing the data, however, is not the end game. The application of the data is the new game.

One innovative IoT application identified was Daimler's Car2Go, which is a new concept for renting vehicles. Among the new features is providing insurance as well as a menu of options to have interconnectivity services with the vehicle. Airbus was another example of a company that is optimizing operations and performance with real-time monitoring of critical components in their aircraft engines. Among the benefits of optimizing operations is to increase the resale value of aircraft by as much as 20–25 percent due to the employment of advanced maintenance features.

Health Care and the IoT

Beth Hoenicke, Senior Integrated Computer Solutions strategist with Johns Hopkins University, discussed many of the advances IoT will make in the health care industry. She

described a digestible pill that when swallowed by a patient would allow a medical service provider thousands of miles away to conduct a diagnostic analysis. She referenced a McKinsey & Company forecast that 40 percent of the Industrial IoT will be in the health care industry. However, there will be a lot of data "exhaust" (pollution) from all the information generated. In addition, the continuing use of legacy technology with IoT will present challenges.

While harmonization of standards is a desirable goal, Hoenicke noted that "one size fits all" is not achievable, so there will be challenges among industrial sectors, as well as between the advanced nations at the forefront of the development of IoT and the less-developed nations to work out standards that will help with interoperability of different platform applications of products.

Encryption

Steve Hanna of Infineon Technologies discussed the use of advanced chips with encryption to help secure IoT products. He noted that while the need for software patches will be inevitable as there is widespread agreement that there is no software code written that does not contain vulnerabilities, the use of encrypted software patches is viewed as a means to prevent reverse engineering of patches and can help prevent counterfeiting by competitors. However, security challenges exist in network systems, software and the cloud.

Infrastructure: OT versus IT

Jesus Molina, Security Consultant, Fujitsu, and co-chair of the Security Working Group for the IIC, discussed the challenges faced by an aging legacy infrastructure. Industrial systems with cyber-physical components were created with security assumptions that are no longer valid. He noted the distinctions between IT and OT and that in the past there was a separation between the two, but they are merging and in a short period of time may be indistinguishable.

With OT, the first priority is safety to prevent injury or death, preserve the public welfare and avoid an environmental catastrophe. The second priority is reliability of the operation of the machinery and infrastructure. Among the challenges is that OT generally has a slower path to an upgrade whereas IT can be upgraded routinely on an almost daily basis. Old technology deployments being married with new technology was also identified as security vulnerability. Older technology deployments will not go away due to the significant capital investment required to develop the new technology deployments. Molina also emphasized that with so many IoT-connected devices and their vulnerabilities to hacking, it is only a matter of time before hackers identify "payloads" that will drive the monetization of the cyberattacks. This pattern is similar to what occurred with the development of PCs and servers. Hackers were initially able to gain access to them, but it took time before they realized the opportunities to secure confidential data and financial information and thereby monetize their criminal activities.

Convergence

The program concluded with a panel discussion moderated by Francis Cianfrocca of Bayshore Networks. The panelists included (1) Tim McKnight, Global Chief Information Security Officer with GE, (2) Demitrios Pendarakis, IBM Watson Group, (3) Brian Witten, Symantec, and (4) Mike Firstenberg, Waterfall Security. The panel discussed the convergence of IT and OT as a crucial challenge faced by the Industrial Internet of Things. OT deals with the maintenance and operations of the machines that are required to run 24/7. The challenge for IT is to monitor and constantly ensure the security of the software program operating the new IoT industrial applications. The two tech teams do not always see eye-to-eye and at times can feel

challenged that each is working at cross purposes to the other's goals. However, without the cooperation of the two, the Industrial Internet of Things will remain vulnerable. Nation state hacking and organized criminal hacking were also identified and discussed as being present threats that will remain threats for the foreseeable future.

The development and deployment of IoT across so many industry sectors is beginning to reveal the patterns of similarities in security concerns as well as the unique challenges that each technology sector will be required to confront as product and service platforms emerge. Meanwhile, the steps being taken by the IIC to establish a framework of open cooperation and sharing of ideas and experiences holds some promise that the inevitable collision of product liability and cyber security issues will be mitigated to some extent. Ideally, as threats are identified, new solutions will be developed and shared across industry sectors.

The Internet of Things: The Cyber Vulnerability Landscape Emerges (March 11, 2016)

The phenomenal growth of the Internet of Things (IoT), widely hailed in 2015, has been greater than originally forecast. Gartner, Inc. estimates a 30 percent increase in IoT devices connected to the Internet in 2016, which equates to 6.4 billion devices, and forecasts that more than 20 billion devices will be connected to the Internet before 2020. On average, 5.5 million new devices are connected to the Internet each day. As the IoT becomes part of the everyday lexicon, there remains a need to examine the myriad risks associated with this explosive growth across multiple industry sectors to address the inevitable weaknesses with software and security that will be part of the foreseeable future of the IoT. In turn, these vulnerabilities can and will lead to property damage, bodily injuries and deaths. Internet attacks leading to physical damage date back to the 2010 cyberattack on the Iranian nuclear energy plant in Natanz that destroyed or disabled centrifuges. Later, in 2014, a German steel foundry was the target of a cyberattack leading to the destruction of a blast furnace.

The vulnerabilities continue to emerge. In January 2016, Forbes and The New York Post reported on a December 23 cyberattack that brought down the energy grid for a large part of the western Ukraine resulting in power losses for a number of cities for a period of several hours. According to published reports, hundreds of thousands of homes and businesses were without power. While not verified, it is suspected that the Ukrainian disruption was, in part, a cyberattack because malware called BlackEnergy was found on computer systems of the affected power companies. The same malware was reportedly found in two other Ukrainian utility companies that were not attacked. On March 1, 2016, The New York Times reported that the Department of Homeland Security (DOHS) issued an alert noting that the BlackEnergy malware was directed to attack the vulnerable industrial control systems.

Perhaps of greater concern, the malware was found to have the capability to permanently delete files and disable the hard drives of the industrial control computer systems. This is precisely where the information technology (IT) and operations technology (OT) for industrial systems intersect and it is the area security experts generally deem to be the most vulnerable to a cyberattack. This is because OT operates 24/7 and does not always synchronize with IT, which frequently provides the perimeter defense against cyberattacks.

Lloyd's of London just months before published a study called "Business Blackout" that forecast the possibility of such an event and addressed the potential economic disruption,

property damage, bodily injuries and deaths that would occur from just such a cyberattack, only this time on a much larger scale targeting the U.S. power grid.

The report studied the potential devastation and economic disruption that would take place if a sophisticated group of hackers (e.g., nation state sponsored or terrorist organization) were able to place malware into the control systems of 50 generators in power plants along the eastern sector of the United States and cause them to self-destruct, thereby sending 15 states as well as Washington D.C. into a blackout. The damage forecasts range from $243 billion to $1 trillion. Page 25 of the report provides a very good discussion on the vulnerabilities insurers presently face, in part because they may have a significant stake in covering the aftermath of such an event but have not realized that their current policy language in the absence of specifically crafted exclusions makes them vulnerable to first-party and third-party claims.

Unlike the U.S. grid, the attack on the Ukraine power grid may have been thwarted by the fact that the country relies on antiquated technology and is not fully connected to the Internet. This allowed the companies to restore power within a short period of time "by manually flipping old style circuit breakers." This, however, cannot be done with the U.S. power grid; thus, a similar attack on the U.S. power grid could have much greater long-term disruptive consequences. However, the vulnerability to malicious hackers is not limited to the power grid. Most of the critical infrastructure throughout the United States from water treatment plants to traffic lights and air traffic control systems are potentially vulnerable to cyberattacks that could wreak havoc and destruction.

James R. Clapper, Director of National Intelligence, appeared before the U.S. Senate Select Committee on Intelligence in February 2016 as part of a report on the worldwide threat assessment by the U.S. intelligence community. The Internet of Things was identified as a threat "to data privacy, data integrity, or continuity of services." [Emphasis added.] In particular, Clapper noted that foreign intelligence services in the future might use the IoT for identification, surveillance, monitoring, location tracking and targeting for recruitment, or to gain access to networks or user credentials.

On the medical device front, in January 2016, the Food and Drug Administration released a draft guide for post-market management of cybersecurity in medical devices. The guide, which carries no weight of law, was developed in part to address cybersecurity throughout the product lifecycle, including the design, development, production, distribution, deployment and maintenance of the device. The draft notes in particular that cybersecurity risks to medical devices are continually evolving and therefore it is not possible to completely mitigate risks through premarket controls alone.

As part of the premarket considerations, it was recommended that manufacturers should establish design inputs for cybersecurity and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis required under 21 CFR 820.30(g). Among the items to be addressed are (1) identification of threats and vulnerabilities, (2) assessment of the impact of threats and vulnerabilities on device functionality and end users/patients, (3) assessment of the likelihood of a threat and of a vulnerability being exploited, (4) determination of risk levels and suitable mitigation strategies, and (5) assessment of residual risk and risk acceptance criteria.

The cyber vulnerabilities recognized include unauthorized access; modification, misuse or denial of use; and unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may impact patient safety.

In line with these concerns, a Southern California hospital was the target of a recent denial of service attack executed against the hospital's computer system, which was held hostage for 10 days resulting in the hospital paying the hackers $17,000 in bitcoin to provide an encryption key. This attack, if taken further, could potentially have led to critical patient care services being compromised. Examples include patient medical records possibly being altered or devices such as infusion pumps, which deliver chemotherapy medication, becoming vulnerable to dosage manipulations. According to a security consultant, there were a number of such attacks last year against health care facilities, and many more go unreported.

In the consumer arena, in January 2016 it was reported that the Nest thermostat, which allows consumers to control the heating and cooling systems in their homes over the Internet from remote locations, suffered a software malfunction that resulted in the battery draining and shutting down the device, thereby ceding control over the heating and ventilation systems connected to it. The result was a series of complaints from consumers about cold homes, possible water pipe damage and concerns about infants being exposed to unreasonably cold temperatures. While a fix was put in place, there is already at least one law firm soliciting potential plaintiffs for personal injury or property damage lawsuits as well as potentially filing a class action.

Other recent IoT-based litigation includes a class action against ToyTalk, Inc.; Mattel, Inc.; and Samet Privacy, LLC d/b/a Kidsafe Seal over claims of Internet security vulnerabilities with the "Hello Barbie Doll." A similar class action has been filed against VTech for vulnerabilities with digital toys that children use to browse the Internet and communicate with each other. The difference with the VTech case is that hackers actually obtained information on almost three million children and parents in November 2015.

As the IoT continues to expand, expect to see more reports of vulnerabilities, successful cyberattacks and, inevitably, physical damage and personal injury losses from defects with software and sensors as well as cyber security vulnerabilities. There is at this time simply no panacea that will address all the potential vulnerabilities with the IoT; nor can anyone accurately predict how the known and unknown vulnerabilities will manifest themselves and what the fix will cost.

The Internet of Things: A Trifecta of Cyber and Physical Threat Risks (June 5, 2017)

The recent WannaCry ransomware cyberattack provided another chilling reminder of the potential disruptive power behind the Internet of Things. Even before the WannaCry attack in May 2017, a distributed-denial-of-service (DDoS) attack on a domain name server provider, Dyn, Inc., took place in October 2016, pushing many popular internet services offline for hours. The Dyn attack, which utilized the malware Mari as the supporting agent, was a sea-change event carried out by hundreds of thousands of internet-connected devices, such as routers, security cameras and DVRs, that rely on default factory user names and passwords coupled with weak or nonexistent security protections. It illustrated that hackers can now target vulnerable low-hanging fruit and turn it into a super botnet to carry out the DDoS attack. One takeaway from the Dyn attack is that the exponential growth of devices coming online, some 5.5 million per day according to Gartner, creates an unparalleled ecosystem for malevolent actors to find and weaponize the Internet of Things (IoT).

The WannaCry ransomeware attack shut down UK hospitals, Russian computers, factories, and multiple businesses and personal interests around the globe. It has not yet been attributed to a specific actor, although North Korea has been identified as a potential perpetrator. According to The Wall Street Journal, Kaspersky Lab ZAO said the malware appeared in 74 countries. Later reports placed the number of countries impacted at 150.

Japan was among the countries that felt the impact of the attack. The Nikkei Asian Review reported 2,000 terminals and 600 IP addresses had been hit. Among these was a computer for the water and sewer services in the city of Kawasaki. The article went on to note, "the use in infrastructure of connected devices, part of the Internet of Things, made room for the attack."

Hiroki Takakura, a professor at the National Institute of Informatics, in the same article noted: "Production and control devices and other equipment are made to match the systems they are used with, so it can be difficult to update them. The attackers targeted systems that still run on outdated operating systems such as Microsoft Windows XP. More users, lately, are unable to apply the latest security updates due to such issues as software incompatibility, which is something of an alarm bell for Internet of Things."

Assessments & Warnings

In the aftermath of the WannaCry attack, cybersecurity experts again emphasized the vulnerabilities of weak or insecure IoT devices. In a posting, 5 Security Predictions for a Post-WannaCry World, Nicole Henderson provided predictions shared by cybersecurity company eSentire. One of those identified was worm-based attacks that could do physical damage: "worm based attacks could unleash physical damage to infrastructure as we move to the Internet of Things."

With the two latest demonstrations, stakeholders need to address security concerns from the ground up. The trifecta of threats has already been documented and demonstrated. The IoT is vulnerable to attacks that can (1) cause physical damage to persons and property, (2) cause a widespread distributed denial of service to servers and computer systems, and (3) deny access to computer systems to secure ransom.

On May 11, 2017, Director of National Intelligence Daniel R. Coates appeared before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment. A section of the report, "Emerging and Disruptive Technologies," identified IoT as one such technology:

> The widespread incorporation of 'smart' devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks. (Emphasis added)

The United States Government Accountability Office (GAO) issued a Technology Assessment report for the Internet of Things in May 2017. Among the challenges the GAO identified are information security, privacy, safety, the need for standards and disruptive

economic issues from the growth of the Internet of Things. The GAO noted it "…has previously reported that cyber threats to internet based systems are evolving and growing. Without proper safeguards, these systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations or launch attacks against other computer systems and networks. The threat is substantial and increasing for many reasons, including the ease with which intruders can obtain and use hacking tools and technologies."

The GAO identified the following types of attacks against the IoT:

- Denial of service
- Distributed denial of service
- Malware
- Passive wiretapping
- Structured query language injection (SQLi controls a web application's database server)
- Wardriving (search for Wi-Fi wireless networks by a person in a moving vehicle)
- Zero-day exploits (software tool that attacks a flaw in a computer system with no opportunity for detection).

The GAO noted that the lack of security controls in many IoT devices occurs in part because many vehicles, equipment and other IoT-enabled devices were built without anticipating threats associated with internet connectivity or the requisite security controls. Furthermore, the GAO noted that many IoT devices are configured with identical or near identical software and firmware that can magnify the impact of successfully exploiting technical vulnerabilities common to all of them.

While recommending that IoT devices should be designed with software update capabilities, the GAO recognized that IoT devices often are designed without software upgrade capabilities or with a cumbersome upgrade process. In addition, many IoT devices may be deployed with anticipated service lives many years longer than typically associated with high tech equipment, making it unlikely that security updates will continue throughout the entire service life.

The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team published a report in January 2017 − Fostering the Advancement of the Internet of Things − that noted:

"…cybersecurity best practices are a new concept for many IoT stakeholders. Mature manufacturers of newly wired devices, such as an appliance manufacturer … may have little to no experience collecting, securing, and protecting consumer data…"

"…start-ups building IoT technologies and interfaces for the first time may focus primarily on getting a product to market, without considering how to protect and secure computer networks or data."

"…different sets of best practices will be relevant for different IoT entities, such as hardware manufacturers/integrators, developers, deployers, and operators."

The report also identified specific areas that may require special consideration, such as devices used by children and autonomous vehicles, noting that "just as there is no easy description for IoT itself, there is no single prescription for IoT security."

Takeaways

So what are some takeaways from the most recent events?

First, the stakeholders perpetuating the growth of the IoT need to focus on security. The Department of Commerce (DoC) provides a good outline of the broad-based steps that need to be undertaken by all stakeholders looking to capitalize on the potential of the IoT. These include the need for flexible, risk-based solutions. In other words, threats and vulnerabilities are constantly evolving; therefore, predefined solutions become obsolete without the creation of cutting-edge solutions.

Second, there must be security by design, not as an afterthought. The approach needs to be holistic and take into account risk assessment during design and testing of products before they are deployed. Vulnerabilities discovered after the product leaves the manufacturer must be addressed with patching and support throughout the life cycle of the product. Regarding addressing technical limitations, the DoC report notes that many IoT devices have "…computationally weak hardware, minimal operating systems and/or limited memory…" Lightweight encryption may be one pathway to an answer for devices with limited computing power.

Just as there is no free lunch, there are no straightforward, surefire ways to address security vulnerabilities in internet-connected devices. Strategic Principles for Securing the Internet of Things from the U.S. Department of Homeland Security echoes many of the recommendations advanced by other federal agencies, including the Federal Trade Commission, the Government Accountability Office and the Department of Commerce. It starts with incorporating security at the design phase, promoting security updates and vulnerability management, building on recognized security practices, prioritizing security measures according to potential impact, promoting transparency across the IoT, and connecting carefully and deliberately.

Expert Opinions in the Age of the Internet of Things: "You're Gonna Need a Bigger Boat" (December 21, 2017)

In my September 2016 blog post, The Impact of the Smart Home Revolution on Product Liability and Fire Cause Determinations, I forecast "dumb products made smart by connecting to the internet will present a new layer of complexity when a failure occurs." When a product fails and causes property damage or bodily injury, experts are frequently tasked with assessing the root cause for the failure, which can lead to a claim or litigation against a potentially responsible third party. In the age of the Internet of Things (IoT) will experts who have knowledge, skill and training sufficient to address potential root cause failures with a "dumb" version of a product have the requisite expertise to address the root cause failure with a "smart" version of the product − and withstand the challenge to their qualifications and methodology in court? The courts are beginning to grapple with this.

In American Strategic Insurance Corp. v. Scope Services, Inc. (D. Md. September 15, 2017), the plaintiff's expert witness was precluded from offering testimony on the standard of care for the installation of a "smart meter" that was the focus of the plaintiff's subrogation action for property damage. The complaint alleged that the defendant's employee was professionally

negligent with the installation and was the direct cause of the fire due to high-resistance contact between the new smart meter and the meter base.

At the close of discovery, the defendant challenged the qualifications of the plaintiff's expert witness with respect to the standard of care for the installation of a smart meter. The defendant argued that the expert did not have specific experience installing electric "smart" meters. In addition, the defendant claimed the plaintiff's expert lacked sufficient knowledge of the industry standard of care. The defendant contended that the expert's general experience in this field was not sufficient to meet the requirements of Rule 702 of the Federal Rules of Evidence.

In reviewing the expert's qualifications, the court found the plaintiff's expert did qualify to testify as an expert in the field of electric meter installation. However, it also determined that despite his qualifications, the plaintiff's expert had to clear an additional hurdle as to the methodology that he used to form his opinions, in order to show that his opinions met the standard for admissibility. The plaintiff's expert had offered a six-step procedure for the preparation and proper installation of the smart meter. The first three steps dealt with preparation for the installation and the last three dealt with the actual installation. During the plaintiff's expert's deposition, he could not identify the factual basis for the six steps he offered as being an accepted industry standard. In fact, he disavowed any knowledge of the industry having used his six-step procedure.

A footnote in the decision reveals that during oral argument, the plaintiff's counsel attempted to claim there was no standard of care as to the installation of smart meters. This obviously contradicted the plaintiff's expert's previous deposition testimony and was recognized by the court.

The court found the plaintiff's expert's opinions amounted to "little more than his personal views on the proper method of smart meter installation." The court noted that the plaintiff's expert's proposed "six-step standard of care" lacked foundation because it could not be tied to any government regulation, industry standard or common practice. The court also noted the expert's opinion was connected to existing data only by the ipse dixit (an assertion made but not proved) of the expert.

The court concluded: "Without reliably supported standard-of-care opinion testimony, the fact finder cannot answer whether the defendant's actions fall below standards commonly held by those in the profession. Unfortunately, [the expert's] testimony at best amounts to his personnel views on what the industry standard of care should be."

Lessons Learned

In the 1975 blockbuster movie *Jaws*, Sheriff Brody, played by actor Roy Scheider, after sighting the great white shark for the first time was so gobsmacked by the enormous size of their prey, he uttered one of the more memorable lines in Hollywood history to Quint, the hired shark hunter – "You're gonna need a bigger boat." So it will be that smart products connected to the internet, where standards may or may not exist for them, pose a new challenge for experts who may have the requisite skills to offer opinions on the dumb version of a product but lack the new skill sets to avoid exclusion when offering opinions on the smart version … or will new experts need to step forward to complement and supplement traditional experts?

STAY TUNED FOR FURTHER DEVELOPMENT

CPSC Takes a Dip in the IoT Regulatory Pool
(April 2, 2018)

The U.S. Consumer Product Safety Commission (CPSC) announced on March 27 its plan to hold a public hearing on May 16 "to receive information from all interested parties about the potential safety issues and hazards associated with internet-connected consumer products," commonly known as the Internet of Things (IoT).

The significance of this undertaking is noteworthy and welcomed. The CPSC in its announcement clearly recognizes that consumer products connected to the internet are "capable of introducing potential for harm (a hazard) where none existed before the connection was established. The consumer hazards that could conceivably be created by IoT devices include: fire, burn, shock, tripping or falling, laceration, contusion, and chemical exposure." Excluded from CPSC purview, but no less potentially problematic to consumers, are personal data security and privacy issues related to consumer IoT devices. Fortunately, the Federal Trade Commission (FTC) is exercising oversight in this particular arena to protect consumers.

Presently, the CPSC does not have specific guidelines for regulating consumer products that are connected to the internet. However, while every product used by consumers that falls under the jurisdiction of the CPSC have safety standards, these do not necessarily address taking an otherwise dumb consumer product (not connected to the internet) and transforming it into a smart product (that is connected to the internet). The challenge is not limited to addressing the overlay of internet connectivity because "dumb products made smart" incorporate all manner of sensors and software as well as apps that enable remote control and monitoring to enhance service and convenience and to collect data for use by the smart-product manufacturers.

The ability of smart products to be commanded and controlled from remote locations coupled with the vulnerabilities presented by products connected to the internet to be hacked and abused by third-party actors is driving the CPSC's concerns.

The CPSC acknowledges as much in the announcement. Focusing on two specific product safety challenges:

First, the agency is seeking "prevention or elimination of hazardous conditions designed into products intentionally or without sufficient consideration, e.g., high-risk remote operation or network enabled control of products or product features."

The second is "preventing and addressing incidents of hazardization" defined as "situations created when a product that was safe when obtained by a consumer but which, when connected to a network, becomes hazardous through malicious, incorrect, or careless changes to operational code." The CPSC acknowledges, "this is a non-traditional area of product safety activity for the consumer product industry and the CPSC."

And there lies the rub. The landscape of consumer products that have or will become connected to the internet is enormous and continues to grow exponentially. Large and small kitchen appliances, voice assistants (Alexa), security cameras, home security systems, consumer electronics, and home heating and cooling systems are just a few existing examples − not to overlook wearables with many more to come.

The challenge with such a large and diverse pool of internet-connected products is to develop a set of guidelines that can address the safety concerns in a meaningful manner, balancing the welfare of consumers without stifling innovation. Security baked into these products at the design stage will be an obvious starting point. However, maintaining security and software updates over the life cycle of different products will prove problematic. Many smart-

home or consumer products have low computing capacity, which does not lend itself to security patches and software updates.

In addition, new threats are being identified. While software and sensors are the focus, it has been shown that hardware is vulnerable, as recently disclosed by Intel. Stay tuned for further developments.

About the Author

H. Michael O'Brien is a partner in the New York Metropolitan offices of the national law firm Wilson Elser. Michael is a co-chair of the firm's Product Liability, Prevention, & Government Compliance practice and leads the Internet of Things (IoT) aspects of Information Governance. He is also a member of the Information Governance Leadership Committee. With more than 30 years of experience in product liability defense, Michael focuses on representing U.S.- and Asia-based manufacturers and distributors as national counsel in litigation, pre-suit investigations, and class actions. He also advises clients on reporting obligations to the U.S. Consumer Product Safety Commission (CPSC) and counsels it on voluntary recall issues. From 1989 through 1992, Michael lived in Japan, managing the firm's Tokyo office and providing counsel to Japanese, Korean, and Chinese clients. While in Asia, he saw first-hand the vast differences between the U.S. and Asian legal systems and recognized the importance of educating foreign clients on the complexities and requirements of U.S. civil practice and procedures. Prior to joining Wilson Elser in 1983, he spent three years as a staff counsel with the New York City office of The Hartford.

Discussion Questions

1. What guidelines could be developed to address safety concerns, balancing the welfare of consumers without stifling innovation? Maintaining security and software updates over the life cycle of different products may be problematic because smart-home or consumer products have low computing capacity, which does not lend itself to security patches and software updates.

2. How will the losses be investigated, and will responsibility for failure of an IoT product prove more difficult to investigate and thus to establish liability? What types of experts will now be called on to play a role in the investigation?

3. Should an autonomous vehicle do anything it can to protect the passengers, even if it means harming other motorists or pedestrians?

4. Who owns the data in the IoT? Who is responsible for security? What steps are necessary to inform and protect consumers' data from unauthorized uses or hacking threats?

5. Should there be reporting obligations for IoT product defects to government safety agencies? Who will be obligated to report? What event may trigger an obligation to report when there is a threat of physical damage or bodily injury arising from an IoT device defect?

6. Should there be Government oversight or self-regulation?

To Cite this Article

O'Brien, H. M. (2018, Fall). The Internet of Things: A mosaic. *Journal of Multidisciplinary Research, 10*(3), 81-104.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 105-107.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Reflection

Achieving Sustainable Development Goal 6 in Disasters: Puerto Rico, Hurricanes, Humanity, and Hope

Cindy M. Figueroa
WaterStep and Polytechnic University of Puerto Rico

Editors' Introduction

This Reflection is the Intervention Professor Figueroa delivered at the United Nations Headquarters in New York City commemorating the 3rd International Day of Women and Girls in Science, under the lead of the Government of the Republic of Malta and the Royal Academy of Science International Trust (RASIT), the United Nations Conference on Trade and Development (UNCTAD), the Permanent Missions of Costa Rica, Hungary, and Vietnam to the United Nations, which organized a two-day forum from 7 to 8 February 2018, focusing on "Equality and Parity in Science for Peace and Development."

Co-sponsors of the commemoration were the Permanent Representations of Argentina, Australia, Colombia, Cyprus, Georgia, Paraguay, Portugal, Rwanda, San Marino, and Thailand Missions to the United Nations as well as the International Labour Organization (ILO), the World Intellectual Property Organization (WIPO), the International Telecommunications Union (ITU), and the International Union for Conservation of Nature (IUCN).

Following is the text of the Intervention she delivered at the 2018 International Day of Women and Girls in Science Forum's "High-Level Panel on Equality and Parity in Economic Empowerment: Multi-stakeholder Engagement." A video of the Intervention is available here.

Message

Do you remember what you were doing on September 19, 2017?

I was teaching an Organic Chemistry Lab course in San Juan, Puerto Rico. I told my students to keep their phones on and let me know when the next weather report was going live.

Category 5 Hurricane Maria hasn't changed course. It will make landfall in the southeast of the island in less than 24 hours.

I panicked. We must get wooden panels or something to cover the windows and doors.

September 20: I woke up by the sound of a metal pipe hitting the street outside. The wooden panels were blown away, water started getting inside the house… so everyone, let's move to the closet.

September 21: It's time to go outside and see what happened. It's time to work. I saw cement poles on the ground covering the main avenue near my house. I saw houses without roofs. I saw debris where there used to be a house. I still see too many tarps as roofs. I saw an unmeasurable number of fallen trees, but I didn't see any leaves. Everything looked burnt. Puerto Rico is now the country with no leaves.

I saw desperation, I saw compassion, I saw tiredness, but I also saw humanity. Incredibly, I saw positivity. I saw strength.

Three weeks after Hurricane Maria devastated our rainforest and our coffee plantations, I volunteered with WaterStep[443] to bring their systems to the most affected areas in the island. Now, we are giving their systems to every municipality in the country, 78 in total, so everyone can have access to safe water. We have also given these systems to clinics and other medical institutions.

We have had challenges. We still must face many challenges, like the lack of proper communication and bureaucracy. But now, almost 70% of these municipalities have the systems not only for now but for the near future. We must be prepared for next hurricane season. We have four months to go.

Thanks to the WaterStep training, I have been able to train more than a hundred people, men and women, around the island, who will also continue to train others. I have seen confidence in trainees when I tell them how to properly use the equipment with a scientific approach. They feel confident getting answers from someone who knows the actual science behind this technology, someone like me: I am a scientist, a doctor, a chemist.

They love how simple the systems are, how they can easily use it under their circumstances.

This is where we must bring our young kids, where the science is needed, where science is having an impact on society. We must let them see!!! That's the best way to encourage true interest in science and technology. But in order to do that, science must be available.

So, scientists: We must be out there talking to people, bringing peace of mind to people in a chaotic world. We must stop for a moment and stop worrying about publishing as many papers as possible and apply our science to the world, in the world, for the world.[444]

I have worked alongside and witnessed women being leaders in the middle of the biggest crisis our country had to endure. They had carried gallons of water to their houses every day, waiting hours to get supplies to their families, and they kept teaching kids under the craziest circumstances. Many humanitarian organizations have been created and led by women after September 20. I have seen so many brave women stepping up to get our country back on its feet.

[443] WaterStep is a non-governmental organization that distributes safe water technology around the world. For more information, go to www.waterstep.org

[444] Editors' Note: Publishing this Reflection was *our* idea, not that of Professor Figueroa.

Women: We get to make the choice if we want to move ourselves and our society forward or if we will wait for someone else to do it for us. I know we can.

Girls and boys: I never thought that when I decided to study chemistry that I would actually study the chemical composition of a meteorite, or study Alzheimer's disease, or as a graduate student, create nanoparticles to treat cancer with non-toxic drugs. *Or* that I'll be helping my country have safe, clean water. With science, you can have so many opportunities to do great things. I have a 3-year-old daughter. I want her to see you as role models.

Right after the hurricane destroyed basically everything in its path, a campaign was launched to help us deal with our wounded soul. Puerto Rico is rising. I don't know if the economy is rising, if the tourism is rising, if the government is rising, but I do know Puerto Ricans are rising, we are rising in our humanity, our empathy, but we are exhausted so I ask the world:

Help us rise together.

About the Author

Cindy M. Figueroa, Ph.D. (cindy.figueroa@waterstep.org), is the Director of Operations-Puerto Rico for WaterStep, and she teaches at the Polytechnic University of Puerto Rico.

To Cite this Reflection

Figueroa, C. M. (2018, Fall). Achieving sustainable development goal 6 in disasters: Puerto Rico, hurricanes, humanity, and hope. *Journal of Multidisciplinary Research, 10*(3), 105-107.

"BLINDSIDED" by Emily Whitsett • Western High School, Davie FL

1-888-373-7888

National Human Trafficking Resource Center

Do your part. See something? Say Something.

Human Trafficking Awareness Poster Contest Sponsored by Soroptimist International of Davie www.sidavie.org

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 111-119.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Reflection

No Right to Have Rights[445]

Stefanie A. Morse

Abstract

This reflection ponders my experience as a law student, engaging in a service learning project for my immigration law course. My professor's description of this client's case[446] indicated that his communication barriers were psychologically based. Prior to law school, I worked as a clinical social worker in New York City, so I hoped my prior experience and education in working with individuals who struggle with psychological difficulties could apply to assisting Francis in articulating a fear of deportation to Iraq in a way that an immigration official could understand that he had a credible fear. Throughout this process, I learned of the darker processes in the United States whereby immigration officials have the discretion to identify folks with communication difficulties, decide whether they have credibility, and ultimately assign value to the life of that individual based on the official's subjective assessment of who deserves protection from persecution and who does not.

Keywords: immigration, persecution, human rights, communication barriers, research, fellowship

Summary

The main part of my reflection focuses on a case my professor presented to our immigration class within the first week. My professor explained some of the perplexing socio-legal issues with which Francis presented. After learning about Francis' demeanor and some of the details of his truly unbelievable story about his life traveling from Iraq, through more than fifteen countries, to the United States. I asked my professor if he had been evaluated by a doctor. After attempting to find and retain a doctor who would conduct a free physical and psychological evaluation on Francis, I volunteered my own set of skills, grounded in my educational and

[445] Editors' Note: This reflection uses legal citation style.

[446] For the purposes of maintaining this client's anonymity and confidentiality, I will refer to this client as Francis.

occupational history as a social worker. Throughout my undergraduate and graduate education, as well as two years of post-master's experience as a hospital social worker, I spent much time developing effective interviewing techniques when conducting mental health examinations. Based on my history, I hoped my experience would be enough to assist Francis in articulating his fears with regard to returning to Iraq. I met with Francis on three different occasions. Based on those meetings, I drafted a declaration based on my clinical assessment, which Francis later signed.[447]

After finishing Francis' declaration, my professor afforded many more opportunities to conduct additional interviews and mental health evaluations on three of her Somali clients, who were all class members of the Somali Class Action Lawsuit.[448] This was a great experience as well, but my reflection will focus on Francis.

Reason for Choosing Project

When I agreed to undertake Francis' case, I did not know much about the relevant law being that the immigration course had just started. However, since the beginning of law school, I have noticed that very few professors discuss the intersections between legal, cultural, and psycho-social issues of our future clients. For example, Francis' psychological defenses manifested as a result of his traumatic experiences in Iraq, and subsequently impeded his ability to articulate his fear of returning. In conjunction with psycho-social issues particular to Francis, the intersection between Francis' cultural history mattered immensely for his credible fear interview because hyper-masculine societies tend to socialize boys and men not to show fear.[449] I hypothesized, based on prior work with homeless Iraqi men and women, that because of the normalization of hyper-masculinity in Iraq, Francis may not be as forthcoming about past persecution as other refugees due to the emasculating nature of many persecutory dynamisms in the Middle East. I investigated this hypothesis throughout interviews with Francis, and corroborated the hypothesis that Francis absorbed these dogmatic ideas, and further, they likely influenced his inability to show or communicate his fear about returning to Iraq to immigration officials, who were also men. Given this cultural barrier, I hoped that interviewing Francis with some perspective on the intersectionality of the legal, social, and cultural issues inherent in Francis' case may answer some of the questions as to Francis' story, and explain some of the behaviors that had initially raised questions in the minds of the immigration officials. Additionally, I knew volunteering to help with Francis' case would equip me with the opportunity to explore the legal rights of "stateless persons" in the context of Immigration and International Law.[450]

---

[447] I did not include the confidential memorandum I produced for this project, due to Francis' plea for confidentiality around the subject matter of the documents.

[448] Jennifer Hansler & Sophi Tatum, *Somalis Mistreated During Deportation Effort, Lawsuit alleges,* CNN NEWS, (Sep. 17, 2017 at 6:01 p.m.), available at https://media.law.miami.edu/clinics/pdf/complaint-immigration-clinic.pdf.

[449] Convention on Rights of the Child, *Advocates for Gender Equality and Equity in Care, Protection and Development of all Children*, UNICEF.org, (Aug. 29, 2007), available at https://www.unicef.org/earlychildhood/index_40749.html.

[450] UNHCR, *Convention Relating to the Stateless Persons,* acceded by 90 parties and 23 signatories (Sep. 28, 1954) available at www.refworld.org/statelessness.html (explaining the leadership role the UNHCR has taken in assisting non-refugee stateless persons as a distinct population of persons of concern); *but see,* David C. Baluarte, *Citizens of Nowhere: Solutions for Stateless Persons in the U.S.*,

Francis' case sounded messy, challenging and somewhat hopeless. I would be amiss if I failed to acknowledge my love for challenge, and Francis' case sounded like precisely that. From my professor's description of Francis' presentation to the sheer desperation professed in Francis' pro se documents, I knew volunteering for this project would provide an opportunity to learn so many different procedural and substantive laws around asylum law and the rights of detainees in the Immigration system, simply because of the amount of legal issues readily apparent in Francis' case.

Last, I wanted to work with Francis because the information about the case suggested that Francis was a person who was struggling. Regardless of the case's aspect of hopelessness, I chose this as my project because it sounded like the United States was getting ready to deport a potentially victimized person. Also, the Trump administration's xenophobic declarations toward persons from the Middle East fueled my fear of immigration officials dismissing Francis as a "bad immigrant" based solely on his nationality.[451] This discussion frustrates me because it alludes to the question, "who deserves humanity and who doesn't?"[452]

I believe that worthiness is an innate quality of all humans and, therefore, has no prerequisites. Upon ruminating on my beliefs in the context of Francis' case, I asked myself, "Does, or should Francis' life matter less than someone with identification documents?" The obvious answer at which I arrived was, "Francis is a human; thus, he deserves a chance to be heard."

With that in mind, I began reviewing the information available to me and researching case law. I hypothesized about the way I should approach Francis in order to overcome previous barriers to effective communication with immigration officers. I hoped to use my prior experience as a mental health professional to assist my professor in her continuing representation of Francis.

Evolving Goals

My goals for this project were initially vague because this was a totally new experience for me, not only as a law student, but also as a clinical social worker. I held off on setting goals until I was able to meet with Francis and gauge his mental state. I hypothesized that, like many people growing up in a country fighting numerous wars, Francis had likely experienced or witnessed tragedies that may or may not have affected his mental state, so my only goal at the outset of this project was to evaluate Francis' mental status and attempt to gain an understanding of his life events.

As the project developed, I was able to set more concrete goals that I hoped to achieve in my meetings with Francis. Additionally, the more I learned about immigration law and the

---

UNHRC White Paper (Dec. 2012), available at https://www.opensocietyfoundations.org/sites/default/files/citizens-of-nowhere-solutions-for-the-stateless-in-the-us-20121213.pdf (asserting that the U.S. has not acceded either treaty assuring to the rights and protections of stateless persons, and articulating the 'disastrous consequences' of inaction on this issue).

[426] *See, e.g.*, Christianna Silva, *Trump's Full List of 'Racist' Comments About Immigrants, Muslims and Others*, N. WEEK, (Jan. 11, 2018, at 7:42PM), available at http://www.newsweek.com/trumps-full-list-racist-comments-about-immigrants-muslims-and-others-779061.

[452] John C. Yang & Vanita Gupta, *The 'Good Immigrants,' The 'Bad Immigrants,' The Deported: The narrative of fear and vitriol must be changed,* HUFF. P. (Aug. 1, 2017 at 12:15PM), available at https://www.huffingtonpost.com/entry/the-good-immigrants-the-bad-immigrants-the-deported_us_5980a7fce4b0d6e28a10eb4c.

circumstances of Francis' case, the more I was able to ask questions directed at extracting answers that might be helpful for my professor's representation of him. For example, after my first interview, our immigration class reviewed the types of relief Francis might be entitled to, if the Board of Immigration Directors allowed for him to undergo a new credible fear interview. We also learned the standard of review for the new evidence necessary to prove Francis' eligibility for a new credible fear interview. This project brought much of the classroom lectures to life and enhanced my understanding of the relief granted when an immigration official concedes that a refugee has a credible fear as well as when such an official cancels removal proceedings in order to comply with the terms of the Convention Against Torture ("CAT"). I also gained an ability to distinguish what relief one gains under CAT, as opposed to the relief one gains under a successful claim of asylum as a refugee fleeing persecution.

Francis arrived on a raft in Puerto Rico in 2016, and asked a civilian to use her phone to call immigration officers and alert them to his entry and intent to seek asylum. Upon review, Francis represented himself during his credible fear interview, and immigration officials found his story unbelievable. In his motion for reconsideration, the immigration judge predicated his denial on the fact that Francis' explanation of how he came to the United States seemed convoluted, vague, and unbelievable. However, upon reading his transcripts with the immigration officers, Francis was consistent in his story, but vague in his description of experiences pertaining to why he was so fearful of being sent back to Iraq.

My first concrete goal was to gather foundational information by constructing a timeline of Francis' life, in order to develop my own understanding of his life events and to develop rapport that would allow Francis to trust me in future interviews. Once I obtained a solid timeline, my subsequent goal was to facilitate a more detailed and difficult conversation with Francis, by prompting him to elaborate on the "persecutory incidences" that could be helpful to his case, and which Francis previously vaguely referred to as "beatings." I wasn't sure whether he would be willing discuss these with me, but it was a follow-up goal.

My last goal for this project was to construct a declaration in the form of an affidavit that Francis could sign. This would provide future reviewing immigration officials with a psychological explanation for the fragmentary nature of Francis' memory and story. I reasoned that if I could assist Francis in articulating his fears of returning to Iraq, this could assist the immigration officers in understanding why his statements were initially so vague, and further assist Francis in overcoming the barriers hindering his ability to communicate a "credible fear of persecution."

Methods and Approach

I chose to use a "mixed-methods" approach in carrying out my project.[453] This enabled me to use the quantitative data from the U.S. State Department and Non-Governmental Organization ("NGO") reports to verify the validity of Francis' narrative. The "mixed methods" framework equipped me with the flexibility to implement evidence-based interview techniques from my literature review, and implement the findings as to the most effective techniques for interviewing trauma survivors. The qualitative data I found useful during this project came from

[453] Judith Schoonenboom & R. Burke Johnson, *How to Construct a Mixed Methods Research Design,* KOLNER MAG. FOR SOC. AND SOCIALPSYCHOL. (69 Supp. 2) pg. 107-131, PMC Web, (Jul. 5, 2017), available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5602001/pdf/ 11577_2017_ Article_454.pdf.

small studies with long interviews. I found this research to be helpful because the outcomes of these studies documented the experiences of trauma survivors and provided in-depth explanations of what interviewers could have done to avoid retriggering them throughout the data collecting process. Because of the in-depth explanations, I extracted very prescriptive advice for my own approach to interviewing Francis.

Due to the time frame in which Francis grew up in Baghdad, Iraq, as well as the psycho-social risk factor of growing up in an orphanage and not having a family, I went into my first interview predicting that Francis had experienced some level of trauma. This, I reasoned, would mean I would need to take my time in building rapport, and plan a few trips to the Glades Detention Center in South Florida to obtain the missing pieces to his story.

Throughout my literature review, significant writings explored the effect Post Traumatic Stress Disorder ("PTSD") might have on a person's ability to effectively communicate. Upon reading these studies, I immediately wondered whether – if I was correct in my prediction of Francis' history of trauma – Francis' PTSD was a factor in his inability to articulate sufficient answers during his credible fear interview and when the immigration judge questioned him under oath. The research explained that the areas of the brain responsible for effective communication become inhibited when a person with PTSD is re-triggered.[454] Further, even if the immigration judge asked Francis questions in a way that did not resemble mockery or lack of seriousness in Francis' situation, the research indicates that Francis' response may have still been fragmentary and vague, due to the detrimental effect trauma has on a persons' memory. The combination of Francis' history of trauma, in conjunction with his constant state of hyper-vigilance, made Francis a very sensitive person to interview from the beginning.[455]

In order to ensure I was maintaining a trauma-informed approach to interviewing Francis, I took a self-imposed assessment to review important factors when approaching clients with unusual trauma histories.[456] I was unsure of how to approach Francis, but the most helpful factor in the success of my approach was staying mindful of my own body language and verbal communications and ensuring all aspects of my presence were engineering and maintaining a safe environment. This was vital to creating and holding physical and theoretical space for Francis to feel safe enough to disclose the particularly horrific details, which he omitted during his first credible fear interview.

In addition to reviewing the evidence-based practices that have yielded the best outcomes for mental health professionals, I meticulously studied and analyzed the growing set of notes I collected on Francis from previous interviews, in order to prepare follow up questions to ask during future meetings and identify questions to ask my immigration law professor. As part of my objective to approach this project with a sensitivity to and awareness of the intersectional issues inherent in this case, I reviewed Human Rights Watch reports and similar outlets that correlated with the dates of Francis' purported time frame in specific regions. I employed this type of comparative research to ensure my questions to Francis fell within the cultural context

[454] Louis Cozolino, *The Neuro-Science of Human Relationships: Attachment and the Developing Brain*, WW Norton & Co., N.Y., (2006) (Explaining that during states of high arousal . . . the area of our brain responsible for speech *becomes inhibited*, resulting in a diminished capacity to construct an accurate narrative).

[455] *Id.*

[456] See, e.g., Klinik Community Health Center ("KCHC"), Is Your Work Trauma-Informed? A Self-Assessment Tool (2013) available at http://mha.ohio.gov/Portals/0/assets/Initiatives/HumanTraficking/2013-is-your-work-trauma-informed.pdf.

from in which he came, and further to ensure I understood the context from which Francis provided answers to those questions. I am not sure if this comparative tactic has an official name, but it was helpful because it highlighted questions I would not have otherwise known to ask Francis in follow-up interviews. My review also showed significant data on the trauma of fleeing ones' home country and psychological consequences of torture. It suggested that a person who has undergone traumatic experiences will likely have difficulties articulating his or her story in a life narrative.[457]

Reflection on the Project

It is troubling that in a credible fear interview, an asylum seeker is more likely to appear "credible" when the immigration official induces flashbacks. It is a psychologically abusive process when a persecuted person has a better chance of obtaining asylum when he or she presents with physical and emotional symptoms of past trauma, to persuade a decision maker with very basic psychological insight (i.e., an immigration judge). I am not sure what the process should be, but I believe it should be kinder than this. If the legal community wants to abstain from instigating additional psychological distress in trauma survivors[458] then the application procedure for asylum should take into account that individuals fleeing to the United States probably did not turn their entire world upside down by moving to another country for a small reason. Although the statistics and data pertaining to the mental health of refugees is scant and inconsistent, the small amount of data available indicates that people fleeing to the United States as refugees or asylum seekers have experienced at least one "seriously traumatic" instance of violence in their home country.[459] This research implicates an opportunity the legal community has to systemically address the issue, by educating legal actors about trauma-informed approaches to communication for lawyers and judges interacting with this largely-traumatized category of people.

Outcomes

For the purposes of constructing an explanation of a person's experience, a "mixed-methods" approach can be extremely helpful. Mixed-methods approach includes implementing methods useful in other successful interviews done in a similar manner, and seeing how the outcomes from your interview align with existing quantitative data, which involves data collection from surveys and censuses. This approach helped with the verifiable aspects of Francis' story. In our second interview, I prompted Francis with the question, "You said you were held captive by the Al Matte army for 45 days, and they 'beat you' every single day. Can you tell me specifically what you mean by 'beating?'" Francis began to shake, while a horrified look came over his face. Francis' physiological response to the quiet, straightforward question I posed spoke for itself, and I would not have known how to hold space for his response, had it not been for the literature I reviewed about conducting interviews on trauma survivors prior to going

[457] Linda Piwowarczyk, *Seeking Asylum: A Mental Health Perspective*, 16 GEO. IMMIGR. L.J. 155 (2001) (noting that torture destroys fundamental human capacities such as the ability to trust and engage in life).

[458] In my perspective, legal actors have a responsibility to not instigate further harm.

[459] Ilene Durst, *Lost in Translation: Why Due Process Demands Deference to the Refugee's Narrative*, 53 RUTGERS L. REV., at 130 (2000).

to the detention center. The trauma he had experienced started to speak for itself through his physical responses, as Francis sat shaking like an earthquake, sitting across the table from me. He tearfully recounted every detail of the torture and persecution he faced at a transient checkpoint, one of many that had surfaced in response to the de-Baathification of Iraq's government.[460] In the moments when Francis disclosed details about the most painful moments of his life, according to the literature, he was more likely to continue his disclosure when I stayed still and quiet.

My approaches evolved as I became more comfortable asking Francis tough questions. My initial approach was to sit with Francis and go at his pace through the information he was willing to disclose. It became clear that instead of answering my posed question, Francis would unconsciously ruminate on a similar topic, to seem as if he had "answered" the question without having to experience flashbacks. This is a common defense mechanism survivors of trauma use to avoid reliving the physical and psychological pain of his past. My approach to these instances involved first acknowledging his non-answer. Next, while acknowledging how difficult revisiting these topics can be, gently redirecting him toward providing direct answers to my posed question.

My approach to showing or communicating empathy changed the more I read about the importance of non-verbal communication. Much of the neuropsychology research indicates that when an interviewee experiences shame as the result of the interviewer's question, the interviewer can communicate empathy more effectively through glances, nods, and facial expressions than through the interviewer's verbal expressions indicating his or her understanding of interviewee's experiences.[461] Maintaining appropriate eye contact with Francis, while staying still and ensuring he was finished talking before I started speaking, were all ways I found to effectively hold space for Francis to recount the painful memories. Further, these gestures were key to his capacity to do so. Francis' reaction to my accidental shifting, crossing my legs, sitting back in my chair (while he was talking), or attempting to ask follow-up questions prior to Francis concluding his answer reflects the effect of small adjustments to my mannerisms. When I accidentally disrupted the boundaries necessary for Francis to feel safe in elaborating on the horrific details, Francis' response, which aligns with the responses of trauma survivors throughout my literature review, was to end his narrative.

The findings of my literature review along with my education and experience as a mental health professional equipped me with the ability to notice and attend to Francis' outward signs of his internal experience. Accordingly, upon noticing Francis' discomfort as a response to my body language, I would adjust the posture or body movements that were (knowingly or unknowingly) communicating a lack of openness. Upon adjusting my posture to align the messages I hoped to communicate, Francis returned to the narrative regarding his abduction and experiences of torture in Iraq. Consistent with my literature review specific to interviewing persons with PTSD, staying mindful of the effects of my posture on Francis' triggers assisted Francis in staying focused and calm while recalling the traumatic events of his past.

[460] Stephen Farrell, *Report Cites Americans for Purging Baath Party Members,* N.Y. TIMES, (Jul. 6, 2016), available at https://www.nytimes.com/live/britain-inquiry-iraq-war/report-points-finger-at-americans-for-de-baathification-policy/.

[461] Reta Herzog, *The Power of Silent Empathy*, ART. ARCH., (Dec. 2016), available at: http://www.nonviolentcommunication.com/freeresources/article_archive/empathic_listening_rherzog.htm.

What I would have done Differently

My law professor named Mr. S[462] as a potential expert to assist Francis in corroborating the details of his story. After the Iraqi government subjected Mr. S to torture, he was able to shed light on the country conditions in Iraq. Mr. S lived in Baghdad for years, spoke to Francis on the phone during one of our meetings. Mr. S subsequently wrote an expert affidavit describing Francis' credibility. I believe the day Francis spoke to Mr. S was the first time Francis stopped questioning his own credibility because Mr. S confirmed the likelihood of the events that took place throughout Francis' life. Thus, if I had to start this project over again, I would involve the Iraqi expert Mr. S earlier and more often. One of the reasons I think Francis could disclose his horrific experiences in Iraq was because of the affirmation Francis found in speaking to Daniel. This was important because Mr. S was asking simple questions about locations, streets, and growing up in a specific province in Iraq, and up until that point, Francis had not spoken to anyone who could confirm his life story's truthfulness. When Francis engaged Mr. S in a tactical conversation, it empowered Francis to believe his own story enough to share it with me in a more complete way, even after immigration officials repeatedly labeled him a "liar." Immigration officials repeatedly denied the truthfulness of Francis's story, which may have indicated to Francis that he was not safe enough or sane enough to share it in its entirety.[463] Mr. S' phone call was a catalyst for a fruitful and more complete interview with Francis during my second visit.

Conclusions

I now know the requisite elements for what to constitutes a "refugee" and what refugees must establish to prove "well-founded fear of persecution."[464] I have read the case law, statutes, and federal regulations. But after multiple reviews of Francis' case, I started to believe that the US never meant for our laws to protect someone like Francis. Upon further research pertaining to my learning objectives, I read about the two Conventions on the Rights of Stateless Persons, and learned the United States has not acceded to either. One article I found explained the United States chose not to accede either treaty because "[they] are contrary to U.S. laws."[465] In the absence of protective measures and procedures in place to facilitate pathways to obtaining legal status for stateless persons, they will continue to be left vulnerable to trafficking, poverty, and discrimination upon coming to or residing in the United States.[466]

This project was useful in bringing the immigration laws to life and giving tangible examples for how to apply the immigration statute and rules. This project also shed much light

[462] I changed Mr. S's name to preserve confidentiality. Mr. S spoke to Francis on the phone, and wrote an expert affidavit for Francis' case, corroborating facts and country conditions Francis described.

[463] Alberta Association of Sexual Assault Services, *Men and Sexual Assault,* AASAS On. Pub., (updated Feb. 2018) (explaining that the major reasons men do not report rape is out of fear being disbelieved, ridiculed, shamed, accused of weakness, ignored, or in the case of heterosexual men, being perceived as gay), available at https://aasas-media-library.s3-us-west-2.amazonaws.com/AASAS/wp-content/uploads/2015/07/Men-and-Sexual-Assault.pdf.

[464] 8 C.F.R. § 1208.13, establishing asylum eligibility.

[465] United Nations High Commission on Refugees, *Convention Relating to the Stateless Persons,* (Sep. 28, 1954), Report published by UNHCR (Dec. 2012), available at https://www.opensocietyfoundations.org/sites/default/files/citizens-of-nowhere-solutions-for-the-stateless-in-the-us-20121213.pdf.

[466] *Id.,* at 6, (Dec. 2012).

on the ways immigration officials treat immigrants and detainees. For example, when I was reading the immigration judge's transcript during Francis' IJ Review, I noticed he essentially ignored the plain language of Francis' story by failing to inquire about its missing pieces. The immigration judge also overlooked the inherent psychological and cultural uniqueness Francis' story warranted. This resulted in DHS placing Francis into expedited removal proceedings because of Francis' inability to translate the persecution he suffered in a way in which the immigration judge could grasp it.

Service-learning projects are incredibly valuable not only because they require student involvement but also because, for those of us who learn through action, it solidifies the rules in the text. In the absence of an experiential learning component, I am rarely able to retain specific information without forcing myself to read the material repeatedly. The hands-on approach to learning was very helpful to me, and I wish this were a requirement throughout all of law school.

The experiential component was so valuable to my learning experience that I hesitate to make a recommendation for changes. I am an experientially-oriented learner, so this type of project really brought the content from the textbook to life. In terms of recommendations, I would love to see the St. Thomas University School of Law coordinate with immigration attorneys in the field to whom the students could be of use. The students could log pro bono hours while gaining experience and shadowing attorneys in their daily work. Additionally, the arrangement could allow for the project to be one that incorporates both experiential learning and shadowing an immigration attorney over multiple settings, such as court rooms and detention centers. Either way, this project was as eye-opening as it was heart-breaking and absolutely enhanced my engagement in the classroom as well as my retention of the content from the readings. I am grateful to have had the opportunity to meet Francis, and I hope a version of this experiential component continues to be a part of future immigration classes.

About the Author

Stefanie Morse, L.M.S.W., is a third-year law student at St. Thomas University School of Law (STU Law). In 2014, she completed her Master of Science and Social Work (MSSW) degree from Columbia University in New York City. In July of 2014, she started working as a clinical social worker at Mount Sinai St. Luke's Hospital. After two years working with vulnerable individuals, she realized her passion for advocacy and started the process of applying to law school. She attended law school to become skillful in effective advocacy. In 2016, she started the journey at STU Law. This service learning project provided an opportunity for her to use skills from her experience as a social worker and knowledge she was learning in her immigration class to assist a stateless man in explaining the traumatic events of his own story to write this reflection about a service learning project. She would like to thank Professor Lauren Gilbert for the opportunities that allowed for these experiences.

To Cite this Reflection

Morse, S. A. (2018, Fall). Reflection: No right to have rights. *Journal of Multidisciplinary Research, 10*(3), 111-119.

"NO RETURNS" by Julian Rush • College Academy of Broward County, Davie FL

1-888-373-7888

National Human Trafficking Resource Center

Do your part. See something? Say Something.

Human Trafficking Awareness Poster Contest Sponsored by Soroptimist International of Davie www.sidavie.org

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 123-129.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Reflection

STU-PACT Legal Research Fellowship: A Reflection

Diego Nicolás Sánchez

Abstract

The STU-PACT Legal Research Fellowship was a result of the semester project requirement of Professor Lauren Gilbert's Spring 2018 Immigration and Citizenship Law course at St. Thomas University School of Law, in Florida. This project is of particular importance because the plight of undocumented immigrants became much worse after President Donald Trump was elected into office. A week after President Trump's inauguration, he signed three anti-immigrant executive orders, one of which essentially turned police officers into immigration agents and significantly led to an increase of immigration arrests in the state of Florida. This reflection describes the implementation of a fellowship that permitted a group of law students to get engaged with a South Florida coalition to brainstorm with community leaders, local government officials, and perform legal research in order to advocate for immigrants' rights.

Keywords: immigration, human rights, social justice, research, fellowship

Introduction

In my Spring 2018 Immigration and Citizenship Law course, I chose to focus my service-learning project on helping to establish the STU-PACT Legal Research Fellowship ("the Fellowship") and supporting PACT (People Acting for Community Together) in its campaign on immigration issues in Miami-Dade County, Florida. PACT is South Florida's largest politically nonpartisan, faith-based, grassroots coalition composed of 38 congregations and 2 university members, one of which is St. Thomas University. To achieve long-term social change, PACT uses the power of large numbers of organized people to hold public officials accountable. Due to its size and clout in the community, PACT has been able to enact major county-wide changes affecting low-to-moderate income families, including doubling Miami-Dade County's bus fleet, increasing school-based healthcare, local hiring ordinances, and eliminating out-of-school suspensions (People Acting for Community Together, 2018a).

Through this project, I was able to apply what I learned in the classroom to a real world situation that required identifying possible policy solutions, and I was able to help plant a seed for a sustainable opportunity for students seeking experience outside of the classroom.

Summary of Project

The seven students who participated in the Fellowship (including myself) were involved in brainstorming with community leaders, meeting with local government officials, and performing legal research in order to advance PACT's immigrant rights' agenda. The community leaders and government officials ranged from Archbishop of Miami Thomas Wenski and Miami-Dade County Public Defender Carlos Martínez to Miami-Dade County Commissioners Sally Heyman and Daniella Levine Cava. PACT's membership identified the topics we had to research. They included the following: (1) the number of individuals taken into custody by local law enforcement for non-criminal acts (such as driving without a driver's license) who immigration officials also detained, or deported, or both; (2) the lack of access to public services for undocumented individuals because of the lack of government-issued identification; and (3) the lack of free, legal immigration defense for undocumented individuals.

The Fellowship specifically required a commitment from students to assist PACT, from February to April, by researching legal issues, attending and presenting at PACT Immigration Committee Meetings, attending immigration research meetings, and preparing for and attending the PACT Annual Nehemiah Action. The students were required to track their pro bono hours and obtain approval by Megan O'Brien, Professor Gilbert, and Assistant Dean for Career Development Lourdes Fernández. The first-year students received community *pro bono* hours, while the second and third-year students received legal *pro bono* hours. In addition, successful completion of at least 35 hours would have satisfied the service component for receiving the Certificate in Immigration Practice.

Goals

The goals of the project were to (1) support PACT by researching legal questions around possible immigration policy solutions, and (2) provide STU law students with hands-on, policy and advocacy experience in collaboration with a local direct action organization. These goals are aligned with a broader vision of institutionalizing a program at the University that would support students and a supervising faculty member to work with existing advocacy organizations in immigration-related policy research and community projects. I chose this project primarily because of my positive past experience with PACT, and because I am interested in the implementation of some sort of school program that would financially support students who may be interested in immigration-related projects.

One of the things I hoped to get out of this project was to encourage other students to engage in local policy discussions and, in particular, long-term social change. I also hoped to broaden my network with like-minded individuals from South Florida who dream of a better world and are willing to make an effort to see it happen. I felt that, by engaging in this project, I would further develop my understanding of immigration law by examining the relationship between local law enforcement and federal immigration officials and analyzing how undocumented noncitizens wind up in detention and become removable from this country. I also

thought this project would enhance my understanding of how local policies could be changed in order to affect broader federal immigration policies in support of immigrants' rights.

Methodology

The Fellowship. The complete methodology was not necessarily predetermined for this project. Even though PACT's work and process was previously established, the formation of the Fellowship required a significant amount of work. On January 17, 2018, Megan O'Brien, PACT's Lead Organizer, joined our Immigration Law class to invite students to participate in PACT's immigration campaign. Megan informed us that students would be involved in doing research, brainstorming with community leaders, and meeting with local government officials in order to advance their immigrant rights' agenda.

When it became clear that I was the only one in the class interested in participating, Anthony Vinciguerra, the Coordinator of STU's Center for Community Engagement, reached out to me to see if there was any other way to encourage students to get engaged with PACT. Anthony stressed that it was an "amazing opportunity" for students to be "part of a serious campaign" that could "possibly lead to some real change," and that PACT really needed the research support. Consequently, on January 30th, Anthony and I met to discuss the possibility of students to earn *pro bono* hours for their work and other ways to incentivize them to support PACT. We discussed the possibility of creating some sort of "research assistant" position, and I also offered Anthony the opportunity for him to present at our following Immigration Law Students Association ("ILSA") General Meeting. Coincidentally, Dorit Matthews, STU's Major Gifts Officer, walked in, and Anthony and I took advantage to discuss with her the idea of a long-term initiative at STU. Before I could process everything, Anthony sent me a draft proposal of a long-term plan a few hours later.

The following week, at ILSA's February 6th General Meeting, Anthony presented on PACT's work and about the overall idea of the Fellowship, and a number of students expressed interest. Therefore, Anthony went ahead and created the Commitment Form of what would later become the Spring 2018 STU-PACT Legal Research Fellowship. The Commitment Form outlined an overview of PACT's work, the potential work of a Fellow, and the approximate hours a Fellow would commit to completing. After several revisions of the form, it was sent to Assistant Dean Fernández for approval.

On February 13th, the final Commitment Form was sent to the law school community, advertising the Fellowship as a partnership between the Law School, the Center for Community Engagement, ILSA, and PACT. On that same day, I began to meet with interested students to discuss the Fellowship and encourage them to sign the Commitment Form. I particularly focused on reaching out to my close circle of friends and colleagues. Among the students who eventually signed the Commitment Form, there were two first-year students, three second-year students (including myself), one third-year student, and one LL.M. student from the Intercultural Human Rights Program. The majority of the students were members of ILSA. Additional meetings and phone calls were required to carry out the project. I was able to document at least eight hours I spent coordinating the Fellowship through initial meetings with the fellows and check-in meetings or phone calls with the rest of the team.

In order to maximize communication and efficiency within the group and hold each other accountable, we created a Google Drive folder where everyone had access to the working documents and was able to see who was working on what assignment and the amount of time

each person would spend on a specific task. The Pro Bono Hours Tracking Log required everyone to document the date, time spent working on an assignment, and the specific tasks performed during that time. In addition to this, we divided the group into two teams – one team worked on the issue of local law enforcement collaboration with ICE (U.S. Immigration and Customs Enforcement), and the other worked on the issue of lack of government-issued identification among the undocumented community. Each team communicated separately via group text-messaging.

PACT. PACT's methodology involves primarily a three-step process, in which every year, its membership: (1) identifies key issues facing its membership, (2) researches concrete solutions to these issues, and (3) advocates, using the power of its numbers, for concrete, long-term policy changes that affect these issues (People Acting for Community Together, 2018b). PACT identifies the key issues through an extensive 'Listening Process' reaching more than 1,500 members. After the listening process, PACT members vote on two to three problem areas to focus on for the year. For the year of 2018, PACT members voted to focus on immigration, affordable housing, and gun violence. The Fellowship was particularly key for steps number two and three of the process, mainly when it came down to narrowing down the focus on immigration areas.

As indicated in the Commitment Form, the following questions regarding local law enforcement and ICE collaboration were our starting point. We were to research them thoroughly and present them at the PACT Immigration Committee Meetings.

(1) Nationally – What cities, counties, and states in the United States have effective policies that prevent local law enforcement officials from collaboration with ICE? What is the policy? Who signed the written policy? How well is it enforced? Are there negative consequences of the policy? Are there any cities in the State of Florida with such policies? (C.F. Tallahassee and Tampa?)

(2) Miami-Dade County – Do any cities in Miami-Dade currently have directives that prohibit local police from collaboration with ICE, or instruct local police to only detain individuals and bring them to the county jail only if their infraction clearly merits this? For example, prohibit local police from detaining individuals for non-criminal offenses (such as driving without a driver's license), or profiling based on potential non-legal immigration status?

- If any of the various municipalities in Miami-Dade County were to draft such a policy, in each case, who would be the official capable of issuing such a directive, and which national model should it be modeled on?

- Finally, clearly describe the shift in county jail detention policies that made it easier for ICE to pick up undocumented individuals who had committed minor infractions and were being detained at the county jail. How could this be changed? Who would be the decision maker, and how could it be monitored and enforced if changed?

In addition to the questions with regard to local law enforcement and ICE collaboration, we were also tasked with researching the issue of too many individuals not having government-issued identification to access certain services (e.g., to open bank accounts, access parks and libraries).

Outcomes

Considering the goals of the project, I believe it was successful in achieving what it set out to do. I feel that I accomplished my goals. The seven fellows were each able to do their part to support PACT by researching the particular questions and helping narrow each issue, and in the process, the project provided the fellows with hands-on, policy and advocacy experience. My initial idea was to be able to recruit two to three students. I never imagined it would receive the interest it did. Even though I was initially worried about students not being interested in the policy or community aspect of the Fellowship, they proved me wrong. The fellows actually enjoyed researching their assigned topic areas, and in particular, the opportunity of interacting and brainstorming with community leaders and local officials.

I have no doubt the project's methodology was effective. By branding this opportunity as a fellowship, students automatically knew it would be something that would stand out in their resumes. Similarly, a few students actually reached out to me about the project simply because they were interested in using it as the service component for receiving the Certificate in Immigration Practice. The fact the Commitment Form specifically laid out a description of the project and expectations was also important. Several students noted that the Commitment Form was very structured and it provided enough guidance to encourage them to sign up. I was very encouraged to see that two first-year students decided to participate.

We did not make many changes along the way. We first started with a group text with all the fellows, but eventually, we noticed it would be more efficient to split the group messaging by topic of research. Also, in the beginning, I served as the liaison between the group and PACT. However, when it became too much to handle, I began directing fellows to simply send emails to the entire group, including the PACT organizers. If I could start all over, I would have perhaps focused on coordinating the group and not being part of the research team. In the alternative, I would have made the group a bit smaller. There were a few instances in which it became too much to handle; yet on other occasions, some fellows either needed more guidance or simply did not have much to work on. Moving forward, I think the best thing would be to implement an application process and make it a slightly competitive so students make an effort and articulate why they would be interested in becoming a fellow.

In total, the group provided over 130 hours of *pro bono* service in two months. We were able to gain invaluable experience by interacting as a team and by having exposure to community leaders and local officials. We did our best to clarify and guide the members of the Immigration Research Committee with our findings. On one occasion, the fellows even had the opportunity to vote to narrow down the research focus and potential asks. One of my favorite things about the outcome of the project is that one of the first-year fellows decided to apply to the immigration clinic and is considering practicing immigration law as a result of participating in the Fellowship. This student was eventually accepted to the clinic.

Conclusions

This project was very useful in providing me a greater understanding of immigration law. I observed firsthand what the power of the community could accomplish if it is well organized. Nearly 1,500 people attended the Nehemiah Action Assembly at Notre Dame d'Haiti Catholic Church, and most of the local officials present committed to helping to solve the issues the assembly highlighted. For example, Commissioner Daniella Levine Cava stated she "will continue to press county staff to complete a feasibility study by September 15 on issuing municipal IDs throughout the county." In contrast, I also learned about the extent to which undocumented Americans are caught up in the net of deportations for simply driving without a valid driver's license. According to the ICE Enforcement and Removals Report from 2017, there were 33,366 more administrative arrests than in 2016 nationwide, representing a 30% increase (Bialik, 2018).

The biggest percentage increases were in Florida, northern Texas, and Oklahoma. The number one arrest category in Florida was "Traffic Offenses - DUI" (total of 80,547) and number four was "Traffic Offenses" (total of 68,346). In 2017, in Miami-Dade County alone, there were 1,215 jail bookings for the offense "No Valid Driver's License."

Service-Learning Component. I strongly believe that incorporating a service-learning component to a course is key to ensure that students apply what they learn in the classroom to the real world, and to encourage them to step out of their comfort zones and learn from the community the same way they learn from the textbooks. The hands-on experience may not only help students retain more information, but it will also add to their "marketability" as soon-to-be lawyers. It will expose students to community organizations and provide them with a glimpse of how life in the real world will be. The value of a service-learning component has the potential to be just as important as an internship opportunity. My experience with PACT is a vital source of information about some of the concepts and issues that we covered in class.

I believe this type of skills-based component can be improved in some ways. It may be insightful to simply allow students to brainstorm on their own early in the semester without even providing them with choices. This may be effective particularly when students are broken down into groups. Some students may be more excited to work on a project when they are doing it with a close friend of theirs or simply with someone who shares a similar interest. I would actually continue to encourage students to work in pairs or in a group. I think it will be helpful to provide some guidance earlier on as to what is expected from the service-learning component. At some time after the breakout session, I think it may be helpful to sit down with each student one-on-one to discuss their idea and provide some guidance. Lastly, I think it is important to provide deadlines early on. Early sets of deadlines will provide students the opportunity to plan their semesters accordingly and avoid any last-minute arrangements for their projects.

References

Bialik, K. (2018, February 8). ICE arrests went up in 2017, with biggest increases in Florida, northern Texas, Oklahoma. *Pew Research Center*. Retrieved from http://pewrsr.ch/2slfPJa

People Acting for Community Together. (2018a). About Us. Retrieved from http://www.miamipact.org/about.html

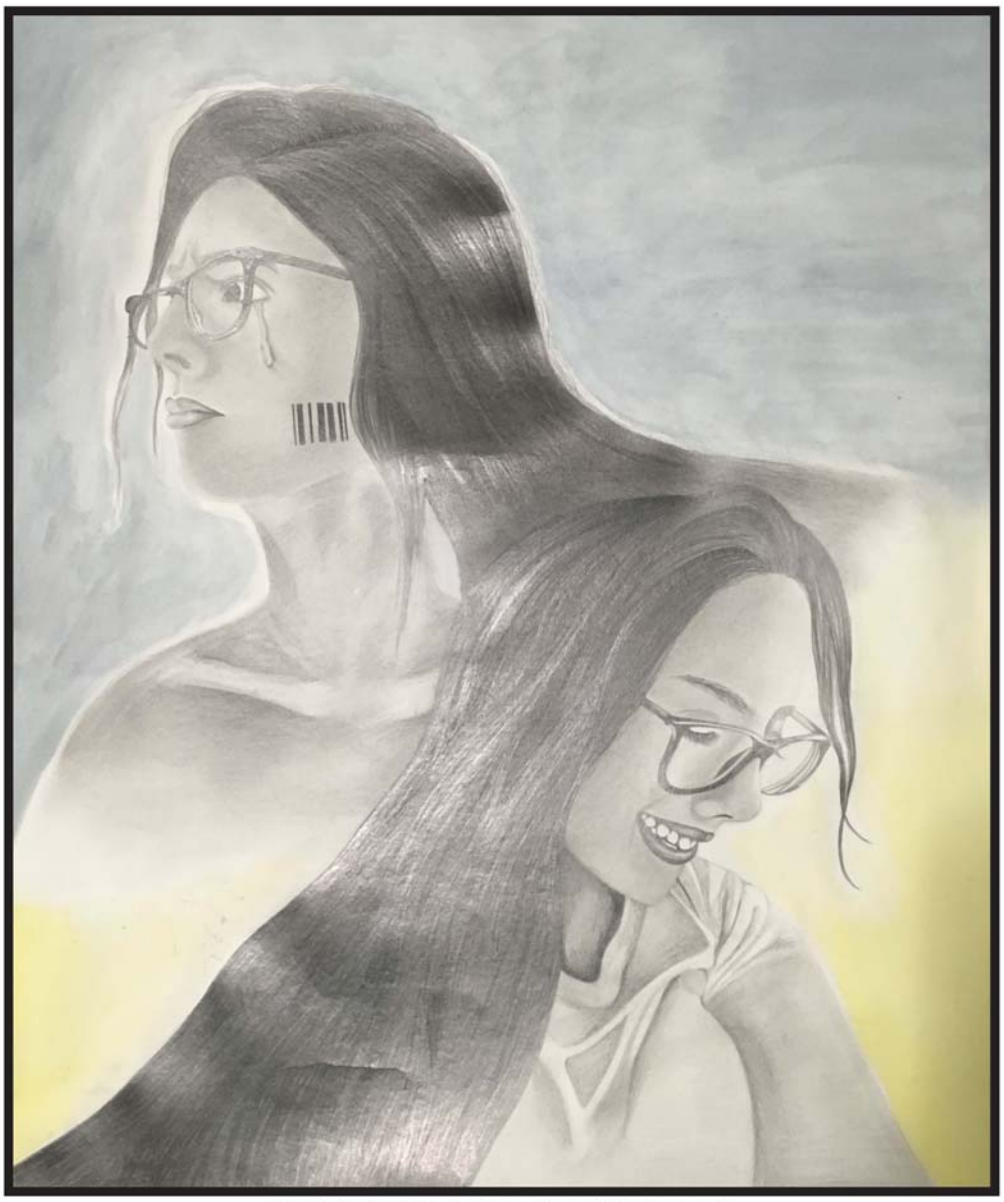
People Acting for Community Together. (2018b). PACT's Annual Process. Retrieved from http://www.miamipact.org/annual-process.html

About the Author

Diego Nicoás Sánchez is a law student at St. Thomas University School of Law.

To Cite this Reflection

Sánchez, D. N. (2018, Fall). Reflection: STU-PACT legal research fellowship: A reflection. *Journal of Multidisciplinary Research, 10*(3), 123-129.



"BEHIND EVERY SMILE" by Wen Cheng • Western High School, Davie FL

1-888-373-7888

National Human Trafficking Resource Center

Do your part. See something? Say Something.

Human Trafficking Awareness Poster Contest Sponsored by Soroptimist International of Davie www.sidavie.org

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 133-137.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Life Forward

Eran Belo: High-Tech Executive

Eran Belo currently serves as a Vice President of Business Development at Adyen, one of the largest payment companies in the world. Born and raised in Israel, Eran left to Australia in 2007 to play soccer after completing a full mandatory army service. He then moved to the United States on a soccer scholarship, starting at West Texas A&M University and graduating with a B.A. in International Business from St. Thomas University in 2011. After graduating, he worked at SafetyPay, a Miami based payment processing company, and volunteered at the Holocaust Memorial of the Greater Miami Jewish Federation. In late 2014, he moved to San Francisco to pursue a great opportunity in the payment industry with Adyen. Eran is a husband, traveler, and avid reader. He claims that his travel experience, multiculturalism, and interpersonal skills led him to build an extensive network, which he makes sure to nurture and grow at every single opportunity. He focuses on being present, continuous learning, and striving to always be in beta mode. Eran is looking forward to seeing what the next years have in store for him and welcomes everyone who reads these lines to become part of the journey.

Interview

by Raúl Fernández-Calienes, Managing Editor
Journal of Multidisciplinary Research

(1) Life is about stories. Do you have a favorite story you use as an icebreaker?

My favorite story is not a typical icebreaker but it gets me emotional every single time.

In June 2015, I was heading to Amsterdam on a work trip. My parents were traveling to Tuscany, Italy, with friends around the same time. I contacted Dani (my parents' friend) and coordinated a surprise visit during the trip. We scheduled a day and approximate time, and I even got in touch with the hosts in the villa where they all stayed. After a long trip from San Francisco→Amsterdam→Frankfurt→Florence, I arrived in a small airport in the late afternoon. I waited few hours in the airport and planned to surprise my parents in the villa during dinner. At 7:30 p.m., I took a taxi to the address I was given by the host and after half an hour I arrived in a place that did not look like the Tuscany villa I imagined at first. The taxi was already two blocks away before I realized I am definitely not in the right place. I knocked on the door of what looked like the most city-like apartment in the Italian country side just to see someone looking through the eye peephole and frantically calling "mom." I would probably do the same if I was him. I immediately called Dani and told him I am lost. While waiting on Dani to respond, I realized I have 10% battery – great! I walked around until I found an ice cream shop, the only place that was open in a town that went to sleep at 6 p.m. I asked the locals about the address just to realize I pronounced the name of the street wrong. One of many times my accent got me in trouble. The right address was about a mile away. Quick look at my carry-on luggage, and my phone made me ask for a taxi. The store owner made a call to a friend, probably the only taxi driver in a town where everybody has a car. A few (loud) words, back and forth, before he hung up and had a bad-news face. Walking it is, then. Luckily, the sun goes down very late in a European summer, though it started getting darker by the minute. I started walking, crossing a rocky bridge and a small part of a highway with a narrow sideline and no light, until I finally arrived to what seemed to be a hilly grape vine. Dinner has started, and Dani found an excuse to be delayed. He gave me a call and put the host on the line, but it was hard to explain where I was when everything looks the same. Google map was eating my battery and apparently not country-side friendly, so I decided to try the oldest trick in the book and knock on the first door I see. However, each house was a mini-castle, so I tried to yell toward one of the big windows just to see a person open, take a look, and shut the fancy French doors. I would do the same – "take two."

After wandering for another 20 minutes, I decided to head back to town and look for a place to sleep. It was pitch dark, I had 2% battery, and my luggage did not seem to enjoy frequent encounters with stones, grapes, and everything you can find in a farm.

I was in the middle of thinking of how it is like to spend a night on a bench and checked on my phone what time is sunrise when a car finally passed by. I was waving with mild urgency, trying not to scare another local. It happened to be my host's neighbor. I am pretty sure my sigh of relief was followed by a tear. I used the very last of my phone's battery to let Dani know I will be outside shortly. The moment of the encounter is a memory I will cherish forever.

(2) What are the top three characteristics that contributed to your success?

- Consistency

Consistency is key. Throughout my time as an athlete, I developed strong stamina to excel at something for a long period without expecting any reward. It then carried to my professional life, where I found myself sticking to the same belief that doing well for a long period of time is a long train tunnel with a beautiful light at the end.

- Passion

The brain cannot function without a heart.

- Stepping outside of my comfort zone

Studying abroad, presenting in front of entire class in a non-native language, applying for a job with only half of the experience needed, getting the job, presenting in front of an entire room of professionals without all the knowledge. Nobody is perfect or knows it all and comfort zones never expand on their own. The first step into my next big thing always included a little stretch and an awkward smile.

(3) What life-changing events or decisions have guided your career?

My move to the US, moving to San Francisco. Moving, in general.

Life is short, and I believe we only get richer by traveling, encountering new places and cultures, and expanding our "mental" horizons. In 2007, I took a bold move and left a cozy hometown and loving family, and a developing career as a soccer player, to pursue my international dream. I lived in Melbourne, Australia; Amarillo, Texas; Miami, Florida; San Francisco, California; and today, I live in New York. I never knew it would turn out as well as it did, but then again, if it would not (or if I felt stagnant) then I would just move again. You have to go places to get places.

I am planning to visit all 50 states before I start my next chapter. To date, I am half way through.

(4) Tell us of any expressions your parents often repeated with you.

My dad always pushed onto me the "attack the awkwardness" (loosely translated). In moments of tension with a teammate, a colleague, or a friend, we tend to take the easier route and not talk about it, but I always had my dad's phrase guiding me when I tackled the situation by facing it rather than pretending everything is alright.

My mom used to tell me that "my openness will unfreeze others." I was always very expressive of my emotions, and thinking of that phrase in the context of this interview takes me back to the origin of this trait.

(5) What books have you read lately?

- *Sapiens* – A must read for every homo-sapiens. For the lazy among us, a movie is coming out soon.

- *The Thread* – Victoria Hislop is my new favorite! Most of her novels take place in Greece, which draws a picture of my grandparents' birthplace. *The Thread* is a beautiful story that made me feel like I am reading it from the point of view of my grandparents, before and during World War II.

- *Cathedral of the Sea* – A classic novel about the Barcelona we will never know.

- *Memories After My Death* – Written by Yair Lapid, who is now running for prime minister in Israel, about his dad's memories from growing up in the holocaust to becoming one of Israel's most influential politicians and figures. I got so emotional reading this book thinking of my dad, who symbolically was the one who gave it to me.

- *A Tale of Love and Darkness* – Had to insert this one as the author passed away on the day of writing these words. Amos Oz is one of Israel's most renowned authors, and this one was my favorite of his. It discusses the days before, during, and after the establishment of Israel and provides an interesting take on life in that era and place. It was later translated into a movie starring Natalie Portman.

(6) Imagine your phone rings and it is you from 10 years ago. If you only had a minute to talk, what would you say? (Yes, I know, Buy AAPL)

In 10 years you will be riding a self-driving car to work, listening to Donald Trump's inauguration speech. Everything is possible.

(7) What elevator speech would you give children about success in life?

Always be authentic because you are the best YOU, and nobody else will ever be a better you, than YOU.

(8) What is the best advice you've ever received, and who gave it to you?

It was at my first work after college. I got very emotional seeing one of my favorite colleagues being let go. I shared my feelings with our Chief Technology Officer at the time, Antonio Rolando, who told me a sentence that would change the way I see things: "People are the architects of their lives." As simple as it may sound, it gave me a different perspective to life's choices, life's circumstances, and life in general. We cannot control the weather or time, but we can determine our future through the actions we take today.

(9) What would you like to see as your life's legacy?

I have two life goals that qualify perfectly in the context of legacy.

- The material one: I want to leave my future child a Patek Philip watch because "You never actually own a Patek Philip, you merely look after it for the next generation."

- The non-material one: I would like to build an orphanage. No street-naming after me or owning a sports team will generate the same satisfaction of assisting a helpless child to have a better future.

(10) Who are the people that contributed to your success the most?

- My grandma

Despite experiencing horrors and death in the family during the Holocaust, my grandma was a woman full of life. In an age of consistent search for fulfillment, which is an oxymoron by itself, she showed me how one can be genuinely happy just by seeing the sunlight through a window or hearing a child's laughter. I learned to appreciate the small things in life, which made me more aware and appreciative of things of higher impact. Absorbing this behavior growing up, I found myself falling in love with my wife (then girlfriend) for similar characteristics.

- My parents

My parents are the type of parents who will give all they got just to feel they have not done enough. I grew up having exactly what I need – love and warmth. The combination of their characteristics made me and my siblings socially aware, ethical, and go-getters. Ever since I remember myself, I was feeling that home is my safe place and that I have total freedom to make my own choices knowing my parents will be standing by me. That is why I will do everything I can to surround my (future) kids with the same kind, protected, and yet liberal environment.

- My college professor

I truly believe we are all surrounded by leaders, influencers, and mentors and those who have not succeeded just did not look hard enough. Dr. Hagai Gringarten was all of the above for me. College is a major junction in one's life. It is the time in which you make the choices that will determine your career and personal path. Dr. Gringarten was my "instrument" for success and the one who was there to give me the perfect hints to achieve success while learning, all over a cup of coffee. Following my college experience with Dr. Gringarten, I am a huge believer that when the student is ready, the teacher will appear.

To Cite this Interview

Fernández-Calienes, R. (2018, Fall). Life forward: Eran Belo: High-tech executive. *Journal of Multidisciplinary Research, 10*(3), 133-137.

”I left my heart in San Francisco”
2019

Photography by Scott Gillig

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 139-140.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Book Review

Book Details

Jorisch, A. (2018). *Thou shalt innovate: How Israeli ingenuity repairs the world.* Jerusalem, Israel: Gefen, 245 pages, $16, paperback, ISBN: 9789652294937.

Reviewer

Thomas F. Brezenski, Ph.D.

Synopsis and Evaluation

As schoolchildren, we all become familiar with the great contributions to the development of modern civilization of the Greeks and the Romans. We are all made aware of the great strides in science, art, and law made during the Renaissance. Those of us who thirsted for more read how various ethnic groups such as the Irish have "saved" civilization. These are all well known and well trodden academic and literary paths by now in terms of the history of innovation and invention. Avi Jorusch, in *Thou Shalt Innovate: How Israeli Ingenuity Repairs The World,* however, unveils perhaps the best kept secret in the modern world: how a tiny nation-state in the powder keg of the Middle East that fights for survival on a daily basis has immeasurably helped improve the global human condition in numerous ways almost no one knows, this reviewer included.

If history has taught us anything, it is that the Jewish people as a rule are tenacious and resourceful after centuries of persecution and ultimate success in carving out the state of Israel. However, most associate the Israelis with success and innovation in the martial and political worlds, and with good reason. The legendary intelligence agency the Mossad is one of the most feared and respected organizations on Earth, and its mere mention is enough to cause the most hardened terrorist pause. Political and military leaders such as Golda Meir and Moshe Dayan are heroes in their respected spheres, renowned worldwide and revered at home. The Israeli military machine, through its victories over aggressive neighboring states and the ongoing fight against terrorism, is regarded by some as the world's best trained and equipped. Jorisch, however, shows the reader a different side of Israel: a kinder, gentler populace dedicated to making the world a better place all the while maintaining the fight for self preservation. I first learned what the Yiddish word *mensch* meant from my Jewish friends when I was boy growing up, and what the author explains is a person of honor and integrity. The title of the last chapter of *Thou Shalt Innovate* is titled "Be A Mensch" and is a perfect capstone to a tome filled with wondrous and uplifting "did-you-knows" in terms of Israeli innovation, which are sprinkled throughout the book. Ever get lost and find your way home through Waze? Thank Israeli inventors. Use online instant messaging? Thank the Israelis again. The book's appendix lists Israel's 50 greatest

contributions to the world, and if you don't read the entire book, it pays just to see the list and be impressed at the tremendous strides a country less than 100 years old has made in the modern world. This reviewer personally recommends reading the entire tome for its inspirational and sometimes downright touching stories of helping make the world a better place for all, even those in the most unfortunate of circumstances such as quadriplegics. Indeed, the story of the paralyzed Israeli doctor who invented an exoskeleton to help the paralyzed walk again is worth the price of the book alone. Anyone who reads *Thou Shalt Innovate* will see Israel in a new and softer light and come away feeling positive about the better angels of human nature in a world increasingly wrought by division, selfishness, and anger. Avi Jorisch has penned one for the bookshelf that this reviewer recommends as a salve anytime one feels worn down by the negative news of the world and needs some bona fide Yiddish literary chicken soup for the soul.

In the Authors' Own Words

"Israel does not have a monopoly on good ideas or proper execution. All countries would benefit from tapping into their own cultures in order to apply their own lessons to the industries and professions they have excelled in for centuries. With this said, the Jewish state's achievements for the benefit of mankind should be celebrated and emulated by the global community" (p. 175).

Reviewers Details

Thomas F. Brezenski (tbrezenski@stu.edu) is an Associate Professor of Political Science in Biscayne College at St. Thomas University in Miami Gardens, Florida. He is a firearms and mental health public policy analyst and serves on the 23rd Congressional District (FL) Gun Violence Task Force. He has taught classes in foreign policy and has reviewed *Doomed to Succeed*, Dennis Ross' seminal work on the diplomatic history of the relations of the United States and Israel as well as the *Comprehensive English-Yiddish Dictionary* edited by Gitl Schaecter-Viswanath, Paul Glasser, and Chava Lapin.

To Cite this Review

Brezenski, T. F. (2018, Fall). Review of the book *Thou shalt innovate: How Israeli ingenuity repairs the world* by A. Jorisch. *Journal of Multidisciplinary Research, 10*(3), 139-140.

Journal of Multidisciplinary Research, Vol. 10, No. 3, Fall 2018, 141-144.
ISSN 1947-2900 (print) • ISSN 1947-2919 (online)

Journal of Multidisciplinary Research

Index to Volume 10 (2018)

Compiled by Raúl Fernández-Calienes

By Author

By Title

To Cite this Index

Fernández-Calienes, R. (2018, Fall). Journal of Multidisciplinary Research: Index to Volume 10 (2018). *Journal of Multidisciplinary Research, 10*(3), 141-144.

About the Journal

Advertising

For information on advertising in the *Journal of Multidisciplinary Research*, please contact the Editor-in-Chief (hgringarten@stu.edu).

Archiving

The *Journal of Multidisciplinary Research* is archived in print form in the St. Thomas University Library and in electronic form on the journal's Website (http://www.jmrpublication.org); back issues are available at that Website. In the event the journal ceases publication, access to journal content will remain viable through both the Library and the Website.

Copyright Notice

Disclaimer

The *Journal of Multidisciplinary Research* publisher, editor-in-chief, managing editor, associate editors, and reviews editor, and the members of the editorial advisory and editorial review committees are not responsible for errors or any consequences arising from the use of information contained in the *Journal of Multidisciplinary Research*; the views and opinions expressed do not necessarily reflect those of the publisher, editor-in-chief, managing editor, associate editors, or reviews editor; neither does the publication of advertisements constitute any endorsement by the publisher, editor-in-chief, managing editor, associate editors, or reviews editor of the products advertised.

Electronic Submissions

The *Journal of Multidisciplinary Research* accepts electronic submissions.

Indexing and Listing

The *Journal of Multidisciplinary Research* is indexed in ProQuest, Cabells, EBSCO, Gale-Cengage Learning, CiteFactor, Ulrich's, de Gruyter (Germany), and Elektronische Zeitschriftenbibliothek (EZB)(Germany). It is listed in the *Directory of Open Access Journals*, AcademicKeys, Cision Directory, EconPapers, Gaudeamus, Google Scholar, Isis Current Bibliography, JournalSeek, Journals4Free, The Linguist List, MediaFinder, NewJour, Research Papers in Economics (RePEc), COPAC (England), CUFTS Journal Database (Canada), EconBiz (Germany), Edanz (Japan), HEC Paris Journal Finder (France), MIAR (Spain), Mir@bel (France), NSD - Norwegian Register (Norway), PhilPapers (Canada), REBIUN-CRUE (Spain), SUDOC (France), ZeitschriftenDatenBank (ZDB) (Germany), and the Open University of Hong Kong Electronic Library (Hong Kong). It is accessible via BASE-Bielefeld Academic Search Engine (Germany), and the NIST Research Library (National Institute of Standards and Technology, part of the U.S. Department of Commerce).

License Statement

Open Access Statement

The *Journal of Multidisciplinary Research* is an open access publication. It does not charge readers or their institutions for access. Our users have the right to read, download, copy, print, search, or link to the full texts of its contents.

Peer Review Process

The *Journal of Multidisciplinary Research* abides by a double-blind peer review process such that the journal does not disclose the identity of the reviewer(s) to the author(s) and does not disclose the identity of the author(s) to the reviewer(s).

Permissions and Reprints

For information on permissions and reprints in relation to the *Journal of Multidisciplinary Research,* please contact the Editor-in-Chief (hgringarten@stu.edu).

Privacy Statement

The *Journal of Multidisciplinary Research* uses the names and e-mail addresses it enters into this journal exclusively for the stated purposes of this journal and will not make these available for any other purpose or to any other party.

Publication Frequency

The *Journal of Multidisciplinary Research* is published three times per year.

Sponsorship

The *Journal of Multidisciplinary Research* publisher is St. Thomas University.

The *Journal of Multidisciplinary Research* sponsor is St. Thomas University.

The *Journal of Multidisciplinary Research* sources of support are the generosity of Professor Craig Reese, Ph.D., and the financial support of the St. Thomas University Gus Machado School of Business.

Submissions Policies

The *Journal of Multidisciplinary Research* does not have Article Processing Charges (APCs) or Article Submission Charges (ASCs).

The Journal of Multidisciplinary Research takes measures to screen for plagiarism, using such software as TurnItIn.

Journal of Multidisciplinary Research content requires the following: (√) Attribution, (√) No Commercial Usage, and (√) No Derivatives.

The Journal of Multidisciplinary Research license statement is available here.

Journal of Multidisciplinary Research authors retain copyright to their work.

To Cite Articles

To cite articles from the *Journal of Multidisciplinary Research,* you may use the following example:

Dunn, M. W., Dastoor, B., & Sims, R. L. (2012, Spring). Transformational leadership and organizational commitment: A cross-cultural perspective. *Journal of Multidisciplinary Research, 4*(1), 45-59.

Submissions

Author Guidelines

The *Journal of Multidisciplinary Research* (JMR) seeks to publish authors who strive to produce original, insightful, interesting, important, and theoretically solid research. Demonstration of a significant "value-added" contribution to a field's understanding of an issue or topic is crucial to acceptance for publication.

All articles submitted to the JMR must be accessible to a wide-ranging readership. Authors should write manuscripts as simply and concisely as possible, without sacrificing meaningfulness or clarity of exposition.

Manuscripts should be no more than 26, double-spaced pages (justified, one-inch margins, half-inch indentations, in Times New Roman 12-point font, *using active voice*), including an abstract (up to 200 words), keywords (up to seven terms), references (with DOI numbers), discussion questions (three to five), and relevant tables and figures (in their correct position in the text, not separate and not at the end of the manuscript), and appendixes (at the end of the manuscript). At his or her own discretion, the JMR editor-in-chief may allow additional space to papers that make very extensive contributions or that require additional space for data presentation or references.

Submission Preparation Checklist

When an author submits his or her manuscript to the *Journal of Multidisciplinary Research* for publication consideration, he or she agrees to abide by JMR publication requirements. Specifically, an author must:

- Agree that his or her manuscript is not under review for publication elsewhere and that he or she will not submit it to another publication during the review period at the JMR.
- Attest that the manuscript reports empirical results that have not been published previously. An author, whose manuscript utilizes data reported in any other manuscript, published or not, must inform the editors of these reports at the time of submission.
- Confirm he or she has not submitted the manuscript previously to the JMR for review. He or she may submit a manuscript that previously was released in conference proceedings, but the editors may view this manuscript less favorably.
- Agree that, during the review process, he or she will take down all other versions of submitted manuscripts (e.g., working papers, prior drafts, final drafts) posted on any Web site (e.g., personal, departmental, institutional, university, archival, working series).
- Agree that his or her submission supports the core values of St. Thomas University (http://www.stu.edu).
- Adhere to the sixth edition of the *Publication Manual of the American Psychological Association* (APA, 6th edition). At the initial stage, the editors tend to review less favorably those manuscripts that do not conform to APA and may return them to the primary author for revision prior to submission to the full review process.
- Submit the manuscript in a Microsoft Word file from which the author has removed the title page, his or her name, and all author-identifying references.
- Submit the manuscript via e-mail to the JMR Editor-in-Chief (at hgringarten@stu.edu).
- Be willing to review submissions to the *Journal of Multidisciplinary Research* by other authors if the JMR Editor-in-Chief calls upon him or her to do so.

Journal of Multidisciplinary Research
http://www.jmrpublication.org

Editorial Review Board

The *Journal of Multidisciplinary Research* Editorial Review Board consists of selected individuals, expert in their field(s), reviewing submissions to the journal and serving for one year.

JMR
Journal of Multidisciplinary Research
http://www.jmrpublication.org