SYRACUSE JOURNAL OF SCIENCE AND TECHNOLOGY LAW

VOLUME 28 SPRING 2013

TABLE OF CONTENTS

State of Emergency: Accessibility to Emergency Communications for the Disabled in Metropolitan Areas
Christopher Tommarello……1

The Quasi-Autonomous Car as an Assistive Device for Blind Drivers: Overcoming Liability and Regulatory Barriers
Dana Mele……26

U.S. Export Control Over Cloud Computing: The Forecast Calls for Change
Ryan Murphy ……65

Review of "Transfer of Nuclear Technology Under International Law: Case Study of Iraq, Iran, and Israel" by Namira Negm
Matt Galante……..93

Review of "Reframing Rights: Bioconstitutionalism in the Genetic Age" by Sheila Jasanoff, ed.
Brianne Yantz……107

The Evolution of E-Discovery Model Orders
Daniel B. Garrie, Esq. and Candice M. Lang, Esq.……121

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 1, PAGE1

State of Emergency: Accessibility to Emergency Communications for the Disabled in Metropolitan Areas

Christopher Tommarello

Abstract

An emergency situation places stress upon everyone involved, and often demands individuals work together to find a solution. Whether the victim, the rescuer, or simply a bystander, all parties are often panicked for survival and try to think quickly to right a wrong. Now, imagine trying to perform in an emergency in bustling New York City with one of your senses disabled. More specifically, imagine having to call for assistance during an emergency to either the police or fire department without having the ability to hear, and without public assistance available for aid. The United States has not fully progressed in terms of emergency situations and communication devices for those with disabilities. This has led to a current situation that threatens the disabled with possible unequal access to emergency communication devices in the near future.

Recent federal cases from the Southern District of New York illustrate the large disconnect that exists between the emergency communication systems available in the city and accessibility for those with disabilities. In *Civic Association of the Deaf of New York, Inc. v. City of New York,* New York City attempted to remove over 15,000 emergency call boxes located throughout the city, which would have eliminated access to emergency communications for the disabled, primarily the deaf. The court held that under the Americans with Disabilities Act ("ADA") the City was unable to remove the call boxes without providing an alternative means of

communication for the deaf, raising questions about whether current technology has outpaced the coverage afforded by the ADA.

This article examines the discrepancies between the ADA and emergency communication systems in the United States, specifically New York City, and highlights the need for the law to be amended to require that as new technology is created for emergency communications, adaptations be made to continue accessibility for those with disabilities. The rise and use of emergency call boxes in New York City, coupled with the *Civic Association* case, demonstrates that without a major change to the ADA it is possible that certain individuals with disabilities will be unable to communicate with emergency services in the future. Changes must be made to afford all individuals the ability to access emergency communication devices.

No individual should be concerned about whether he or she will be able to access emergency services during an emergency simply because of a disability. Instead, all individuals should feel secure knowing that in the time of need they are able to access those who can provide help and ultimately relieve a stressful situation.

Table of Contents

I. Introduction……..……....4

II. Americans with Disabilities Act……..……....5

III. Emergency Communication Systems in New York City……...……8

A. Emergency Call Boxes…….8

B. Public Payphones for Emergency Communication……..……10

C. New Emergency Communication Methods…..……..……12

D. Decline in Use of Emergency Call Boxes in New York City……...…….13

IV. Civic Association & Case Law on Emergency Communication for the Disabled…..…….14

A. *Chatoff v. City of New York*……...…..……..15

B. *Civic Association of the Deaf of New York, Inc. v. Rudolph Giuliani, et al.* ……...……..17

C. *Civic Association of the Deaf of New York, Inc. v. City of New York*……29

V. Implications from Civic Association & Predictions……..……21

VI. Conclusion……...……..24

I. Introduction

There is a universal need for assistance through effective communication during emergencies across the globe and particularly in the United States. An emergency typically places individuals in extremely vulnerable circumstances, and creates a dependency for assistance that can usually only be filled by an outside source, detached from the person and the situation. Whether these services come from public entities, like the United States government, or from private groups, such as local firefighter troops, every society needs effective communication methods for providing assistance to those in need. Among major industrialized nations, the United States stands at the forefront of providing emergency communication services to those in need through public assistance programs like 911 and private entities like the Red Cross. Through both its public and private entities the nation has created assistance systems that allow individuals to receive help during times of struggle, and hopefully throughout recovery as well.

However, although the United States has come far in developing emergency communication services for those in need, the nation still needs to develop in the area of providing assistance to individuals with disabilities. In a society that is constantly changing how it provides emergency services based on new technologies, the United States needs to ensure that as emergency services develop and newer methods become available, those with disabilities are still afforded access to these services. In recent years there have been vast improvements in the manner in which emergency communication is done in major metropolitan cities, with large improvements particularly occurring in New York City. With these huge changes occurring seemingly overnight, it appears there are holes developing within the emergency communication systems that the government provides and compliance with the Americans with Disabilities Act

("ADA"). These gaps often leave individuals with disabilities unable to access services in times of emergencies.

One large example of this gap between emerging communication systems and the ADA is the recent federal case from the Southern District of New York, *Civic Association of the Deaf of New York, Inc. v. City of New York* ("Civic Association"). In *Civic Association*, New York City attempted to remove over 15,000 emergency call boxes, which would have eliminated access to emergency communications for the deaf. The court held that under the ADA the action was prohibited.[1] *Civic Association* demonstrates that to account for the inconsistencies between emergency communication systems and ADA compliance, the ADA must be amended to require that as new technology is created for emergency communications, adaptations are made to allow accessibility for those individuals with disabilities.[2]

II. Americans with Disabilities Act

In determining where the gaps exist between current and developing emergency communication systems and the ADA, and how these holes can be filled, it is important to understand what exactly the ADA is and what is covers. All fifty states have statutes that address disability rights that in general prohibit discrimination based on disability, and require that individuals with disabilities have access to the same goods and services as other individuals.[3] The ADA is federal legislation that was enacted in 1994 to create a unified approach to disability

[1] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182 (S.D.N.Y. Nov. 29, 2011).

[2] Sharona Hoffman, *Preparing for Disaster: Protecting the Most Vulnerable in Emergencies*, 42 U.C. Davis L. Rev. 1491 (2009).

[3] *Id.* at 1528.

rights by "[forbidding] public and private entities from discriminating against those with disabilities."[4] In essence, the ADA took a unified stance against discrimination for disability and took what all fifty states were already doing and made federal legislation.

Prior to the passage of the ADA, Congress enacted the Rehabilitation Act, specifically Section 504, which stated that a qualified individual with a disability may not be discriminated against or denied benefits by programs and activities that receive federal funding.[5] Although the Rehabilitation Act was an enormous stride in protecting those with disabilities and eliminating discrimination, the Act did not fully protect individuals with disabilities so the ADA was created to fill these inadequacies.[6] Congress recognized that those with disabilities were being discriminated against in the workplace, all levels of education and numerous other facets of life, and enacted the ADA to try and eliminate discrimination and negative stereotypes while forcing both private and public entities to provide accommodations for those with disabilities.[7]

There are three titles within the ADA that cover different segments of life including workplace and education, and apply to different entities such as the private and public sector.[8] The main segments of the ADA for this discussion, on emergency communications provided by the government, are Title II and Title III. Title III applies to private entities that provide a public service, an example of which would be a privately owned hospital that provides emergency

[4] Hoffman, *supra* note 2, at 1522.

[5] *Id.* at 1524.

[6] *Id.*

[7] *Id.* at 1522.

[8] Hoffman, *supra* note 2, at 1522.

health care through an ambulance or emergency room to the public.[9] Title II applies to public services that are run by a public entity and are used by the public, an example of which is emergency call boxes in New York City.[10]

An individual with a disability is covered under the ADA and can bring a suit against a private or public entity if the person can show that he or she was treated differently due to their disability, and if the treatment was based upon stereotypes or misconceptions about the disabled.[11] In relation to emergency communications provided by the government or state entity, a potential plaintiff would need to show that during or in an emergency a person with a disability did not have a sufficient communication with emergency services based upon their disability, and was therefore treated differently and discriminated against.[12]

Additionally, the ADA includes a compliance manual that specifically relates to public entities and providing emergency communication.[13] Under Title II, telephone emergency services must provide direct access to individuals with disabilities who use public payphones or emergency call boxes. This requirement applies to basic emergency services, including fire, police and ambulance. Direct access means that the communication goes directly to the emergency service without going through a third party.[14] Operators should be trained to recognize that silent calls may be from these services and individuals with disabilities, and be

[9] Hoffman, *supra* note 2, at 1522.

[10] *Id.*

[11] *Id.*

[12] *Id.* at 1523.

[13] Hoffman, *supra* note 2, at 1523.

[14] *Id.*

prepared to assist any type of person or disability.[15] Under this compliance manual, the public entity is also responsible for the implementation, operation and maintenance for adequate number of telecommunication devices for the deaf ("TDD") telephone lines and stations.[16] Title II of the ADA does not require telephone emergency services be compatible with all formats for non-voice communications, rather at least one must be capable of allowing an individual with a disability to directly contact emergency services.[17] With a background of the ADA and what it covers, it is easy to see where the implementation of new technology, specifically New York City emergency call boxes, has led to gaps in providing adequate access to emergency communication devices and compliance with the ADA.

III. Emergency Communication Systems in New York City

A. Emergency Call Boxes

New York City is one of the nation's largest metropolitan areas and one of the best examples of how technology has advanced in the area of emergency communications while maintaining issues in complying with the ADA. Like most major metropolitan cities in the United States, NYC has in place numerous methods that allow citizens to contact emergency services. Currently NYC has over 10,000 emergency call boxes throughout the city that are used

[15] Hoffman, *supra* note 2, at 1523.

[16] *Id.*

[17] *Id.*

by citizens during an emergency.[18] These boxes are located sporadically throughout the city, but are usually not more than one or two blocks from one another.[19]

The boxes come equipped with two buttons, a red one that is used to contact the fire department and a blue one that is used to contact the police.[20] Some of the boxes also come equipped with levers instead of buttons that can be pulled to contact the Fire Department of New York ("FDNY"), however these boxes do not have a two-way communication system like the push button boxes.[21] These emergency call boxes are located on every other street corner and on highways and bridges as well as in public buildings, schools, hospitals, day care centers, prisons and the United Nations buildings.[22] Finally, all of the boxes are inspected and checked daily to ensure they are in proper working condition.[23]

When either of the two buttons is called on the push button box, the user is automatically connected to a dispatcher and allowed to speak directly with him or her to describe the nature of the emergency and what specific services are needed.[24] The user's call must be answered within ten seconds by a dispatcher, and if not, then either the fire department or the police will

---

[18] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *2 (S.D.N.Y. Nov. 29, 2011).

[19] *Id.*

[20] *Judge Forbids City From Removing Emergency Call Boxes*, TRANSPORTATIONACCESS.COM, http://www.nyctransportationaccess.com/news/2011/10/judge-forbids-city-from-removing-emergency-call-boxes.html (last visited Feb. 29, 2012).

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *3 (S.D.N.Y. Nov. 29, 2011).

automatically be sent to the location of the call box depending on which button was pushed.[25] A call can only be canceled if the dispatcher speaks with the user and the user cancels the services, otherwise services will automatically be sent.[26] Finally, the emergency call boxes are supposed to come with vibrations from the buttons when one is pushed indicating to a user who is deaf or hard of sight that the box is successfully working and that the call has been made.[27]

B. Public Payphones for Emergency Communication

Another service exists within New York City for communication during emergencies through the use of public payphones. The private entity Verizon Wireless works with the New York City Department of Information Technology to automatically report the location of the payphone to the dispatcher when an emergency call has been made.[28] This allows someone in an emergency to have emergency services, such as the police or fire department, sent to the user automatically even if they are unable to communicate directly with the dispatcher.[29] Currently the New York City Department of Information Technology and Communication runs roughly 14,500 payphones located in New York City, but they are not located in the parks, subways or in private property or buildings.[30] The phones are evenly distributed throughout the city, but in

[25] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *3 (S.D.N.Y. Nov. 29, 2011).

[26] *Id.*

[27] *Id.* at *4.

[28] *Id.*

[29] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *4 (S.D.N.Y. Nov. 29, 2011).

[30] *Id.*

recent years due to the heavy individual use of personal mobile telephones the installation and number of working payphones is in decline.[31]

Although there are numerous payphones throughout NYC, there is one major downfall with using them during an emergency, that being they are inaccessible to certain individuals with disabilities.[32] A person who is deaf or hard of hearing must rely on speaking with a dispatcher to successfully use a payphone during an emergency.[33] Unlike the emergency call boxes, which send emergency services simply by pushing a button, a dispatcher will only send an emergency service if the user has indicated that he or she needs one.[34] This prevents a person with a disability from being able to independently call for services without the assistance of another during an emergency, which is often difficult to do.[35] The payphones do not come equipped with telecommunication devices for the deaf that enable a person who is deaf or hard of hearing to successfully communicate with a dispatcher, making them inaccessible and essentially useless during an emergency.[36]

---

[31] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *3 (S.D.N.Y. Nov. 29, 2011).

[32] *Id.*

[33] *Id.* at *5.

[34] *Id.*

[35] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *5 (S.D.N.Y. Nov. 29, 2011).

[36] *How Those in the Deaf and Hard of Hearing Community Can Request Police/Fire/Medical Assistance from Public Pay Phones or Emergency Call Boxes*, THE MAYOR'S OFFICE FOR PEOPLE WITH DISABILITIES, http://www.nyc.gov/html/mopd/downloads/pdf/emergency.pdf (last visited Feb. 29, 2012).

C. New Emergency Communication Methods

In recent years, the New York City Police and Fire Departments have strived to develop a new technique to accommodate those with disabilities who are using either public payphones or emergency call boxes.[37] This new method is referred to as the "tapping method," and allows users with a disability to communicate with dispatchers about an emergency through both payphones and emergency call boxes.[38] In an emergency, the user would use a continuous tapping pattern on the emergency call box buttons or on the payphone to indicate what type of emergency services are needed.[39]

For example, if a person needed the NYC police, he or she would dial 911 on a public payphone, wait four seconds and then start tapping the mouthpiece of the telephone in a continuous pattern (TAP TAP TAP TAP TAP) for at least 90 seconds or preferably until the services needed arrived.[40] If a user needed emergency medical services ("EMS") or the Fire Department then he or she would do the same thing except use a two-tap pattern (TAP-TAP pause TAP-TAP pause) to indicate that those services are needed instead of the police.[41] The same tapping patterns are used on public payphones or emergency call boxes, allowing an individual with a disability to contact services in the same manner consistently throughout NYC.[42] As previously mentioned, the NYC payphones automatically tell a dispatcher where the user is located and if dialing 911 the call is free for all users, making it more efficient for users to

[37] THE MAYOR'S OFFICE FOR PEOPLE WITH DISABILITIES, *supra* note 36.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] THE MAYOR'S OFFICE FOR PEOPLE WITH DISABILITIES, *supra* note 36.

[42] *Id.*

receive assistance under this new method.[43] Although it appears that NYC and metropolitan areas throughout the United States have multiple methods to provide emergency services, there has been a decline in the use of these services while an increase in newer technologies that have left gaps between current systems and compliance with the ADA.

D. Decline in Use of Emergency Call Boxes in New York City

Although the emergency call box and other communication systems have been widely used in NYC for numerous years, recent changes in emergency communication services have led to a decline in their use and a gap between emergency services and ADA compliance. To begin, the heavy use of mobile phones by individuals in major metropolitan areas and across the nation has led to a decrease in the use of the emergency call boxes in NYC.[44] In 1999 there were 42,000 emergency call boxes in use and active in NYC, by 2009 that number decreased to roughly 13,000.[45] The majority of individuals now have personalized mobile phones that they use during an emergency to dial either 911 or any other service that is needed, which has led to fewer people using the emergency call boxes in NYC.[46] It costs the city on average $7 million a year to maintain the emergency call boxes, and the city has estimated that over the next ten years it could cost them nearly $24.8 million in maintenance, a cost they do not want to spend if individuals are using cell phones during emergencies instead of the boxes.[47]

---

[43] THE MAYOR'S OFFICE FOR PEOPLE WITH DISABILITIES, *supra* note 36.

[44] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *4-5 (S.D.N.Y. Nov. 29, 2011).

[45] *Id.*

[46] *Id.*

[47] *Id.*

Additionally, because it takes a mere pushing of a button to summon a dispatcher and because after 10 seconds the dispatcher automatically sends assistance to the location of the call box, the number of false alarms for both police and fire department services has steadily risen.[48] In 2009 alone, nearly 11,000 false alarm calls came from the street emergency call boxes.[49] The call boxes were also responsible for 2.7% of the FDNY's incoming calls in 2009, and responsible for 43.3% of the malicious false alarms burdening the FDNY.[50] These false alarms create an issue for the NYC police and fire departments by taking time away from real emergencies and sending emergency vehicles through the bustling streets of NYC at incredibly fast speeds, which has a higher rate of injury to bystanders.[51] Although the emergency call boxes have numerous positive effects to using them, there still exist numerous downfalls and new problems created as technology continues to develop in the area of emergency communication services.[52]

IV. Civic Association & Case Law on Emergency Communication for the Disabled

As previously mentioned, the Civic Association case is a recent example of the manner in which cities and states are implementing new emergency communication technologies, and in doing so creating gaps in compliance with the ADA. However, prior to the ADA there have been

[48] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *2 (S.D.N.Y. Nov. 29, 2011).

[49] *Id.* at *7.

[50] *Id.*

[51] *Id.*

[52] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182, at *7 (S.D.N.Y. Nov. 29, 2011).

numerous cases and precedent that have worked to eliminate discrimination against those with disabilities in emergency communications. In order to identify the inadequacies of newer emergency communication technologies and compliance with the ADA, it is fundamental to understand the background of case law leading the most recent Southern District of New York Civic Association decision.

A. *Chatoff v. City of New York*

In 1996, the United States District Court for the Eastern District of New York held that all public entities must provide individuals who are hearing or speech impaired with the ability to access 911 emergency services.[53] The court held this decision as part of the ADA mandate that public entities must use forms of communication such as TDD and Baudot formats to give access to those with disabilities in public settings during times of emergencies.[54] Direct access meant that a high number of TDD phones and systems should be located throughout the city and operable for individuals with disabilities.[55] The TDD and Baudot methods were already heavily used in other major metropolitan areas across the United States, and the court indicated that if the technology exists in other parts of the country there is no justification for it not being provided in NYC, one of the nation's largest and busiest cities.[56]

The court noted in its decision that the Department of Justice rules state that a person with a disability must have direct access, meaning a person with a disability should be able to contact 911 services directly and not have to use a separate seven digit number to call and

[53] Chatoff v. City of New York, No. 92 Civ. 0604 (RWS), 1992 WL 202441 (S.D.N.Y. Jun. 30, 1992).

[54] *Id.* at *2-3.

[55] *Id.*

[56] *Id.*

indicate that they are a person with a disability.[57] As the House of Representatives noted, those with disabilities must be able to contact emergency services in the same manner as those without disabilities to create equality among members of society and to provide all individuals with the same opportunity to receive help in an emergency.[58]

Ultimately, in *Chatoff*, the court held that New York City had to make all of its 911 equipment accessible to those with disabilities within a certain time frame with the costs of doing so being apportioned to the city.[59] The court also held that the city must train its 911 dispatchers and any other individuals involved in emergency communication services how to better respond and interact with those with disabilities, mainly the deaf, and those involved must be trained in TDD and Baudot techniques.[60] Finally, the court held that the city must maintain all of the emergency communication systems in the city in proper working condition, including the TDD and Baudot systems and more importantly be aware of upcoming trends, changes and best practices for 911 response systems for the disabled.[61] *Chatoff* stands as an excellent example of the manner in which case law is changing and how more courts are finding that public entities must provide accommodations that create equal access to emergency communications for both the disabled and non-disabled. The case was one of many that began demanding that changes be made to allow those with disabilities to contact assistance during times of emergencies.

---

[57] *Chatoff*, 1992 WL 202441, at *2-3.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Chatoff* at *2-3.

B. *Civic Association of the Deaf of New York, Inc. v. Rudolph Giuliani, et al*

In the most recent case spurring discourse on emergency communication systems, *Civic Association of the Deaf of New York, Inc. v. City of New York*, New York City authorities attempted to remove all emergency call boxes in the city and were ultimately prevented from doing so by a federal court in the Southern District of New York.[62] However, prior to that ultimately prevailing case, *Civic Association of the Deaf of New York City, Inc. v. Rudolph Giuliani, et al* ("*Giuliani*") had attempted to prevent the city from doing the same action and was unsuccessful.[63]

The *Giuliani* case was a federal class action lawsuit originally filed in 1995 by an organization of deaf and hard of hearing New Yorkers who were concerned about the city removing the emergency call boxes and being unable to receive help from sources such as payphones during an emergency.[64] Robert B. Stulberg was the lawyer for the advocacy group Civic Association of the Deaf of New York City and represented the group against Mayor Bloomberg, the Fire Department of New York and the City itself in their original complaint.[65] Under the ADA, the class asked the Federal court to block a plan by the City of New York to remove fire alarm boxes from city streets, which would have essentially eliminated the deaf and

[62] Civic Ass'n of the Deaf of New York City, Inc. v. City of New York, No. 95 Civ. 8591, 2011 WL 5995182 (S.D.N.Y. Nov. 29, 2011).

[63] *Civic Association of the Deaf of New York City, Inc. v. Rudolph Giuliani, et al.*, CENTER FOR CONSTITUTIONAL RIGHTS, http://ccrjustice.org/ourcases/current-cases/civic+association+of+the+deaf (last visited Feb. 29, 2012).

[64] *Id.*

[65] TRANSPORTATIONACCESS.COM, *supra* note 20.

hard of hearing from being able to communicate with emergency services as they are often unable to access public payphones.[66]

In February of 1996, the court ruled the group of deaf and hard of hearing individuals as a class and in July of 1997 issued a ruling that the city must restore any alternations that were made to the emergency call boxes in an attempt to remove them.[67] The 1997 court order also prevented the city form removing the street alarm boxes because it violated the rights of the deaf and hard of hearing.[68] The court ruled that public payphones, the city's alternatives to alarm boxes, did not allow the deaf and hard of hearing to access emergency services from the street.[69] The court further found that asking a person with a disability to use a public payphone did not allow the user to indicate what kind of emergency he or she was having like emergency call boxes do, and could lead to a waste of resources or the wrong help being sent.[70]

The court relied on Title II of the ADA, the title that focuses on the actions of public entities, and held that when the government changes an existing public service, the changes must not discriminate against people with disabilities.[71] The court granted the class an injunction stopping the removal of the boxes and forcing the city to replace or fix any of the boxes that were either removed or deactivated.[72] None of the emergency call boxes could be eliminated or shut down and any that had been removed had to be replaced. Any that were switched to one-

---

[66] CENTER FOR CONSTITUTIONAL RIGHTS, *supra* note 63.

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Civic Ass'n of the Deaf of New York City, Inc.*, 2011 WL 5995282, at *10-13.

[71] CENTER FOR CONSTITUTIONAL RIGHTS, *supra* note 63.

[72] *Id.*

button had to be changed back to a two-button system.[73] Finally, the court held that in the future the city might be able to switch to a newer system for emergency communication; however that system would need to be proven effective and accessible for those with disabilities.[74]

C. *Civic Association of the Deaf of New York, Inc. v. City of New York*

In the 2010 Civic Association case, New York City filed a motion asking the court to end the injunction from the Giuliani case and allow the city to remove the 15,000 accessible street emergency call boxes.[75] New York City maintained that the use of the boxes has decreased by nearly 90% over the past 15 years, nearly nine in ten calls from the boxes are false alarms and that it costs the city roughly $9 million to maintain the boxes each year.[76] The city argued that the deaf and hard of hearing can use public payphones and the tapping system to access emergency services and save the city money that it uses every year to maintain the boxes.[77] The city also argued that the boxes result in numerous false alarms and waste the city's resources on sending emergency vehicles and create additional liabilities by having fire trucks and police cars racing through the crowded streets to emergencies that do not exist.[78]

---

[73] *Civic Ass'n of the Deaf of New York City, Inc.*, 2011 WL 5995282, at *2-3.

[74] *Id.*

[75] CENTER FOR CONSTITUTIONAL RIGHTS, *supra* note 63.

[76] Javier C. Hernandez, *City Renews Effort to End Use of Street Alarm Boxes*, N.Y. TIMES (June 20, 2010), *available at* http://www.nytimes.com/2010/06/26/nyregion/26alarms.html (last visited Feb. 29, 2012).

[77] CENTER FOR CONSTITUTIONAL RIGHTS, *supra* note 63.

[78] *Id.*

The motion was argued in United States District Court Judge Robert Sweet's courtroom on June 3, 2011 and August 15, 2011 with the court ultimately finding against the city.[79] The city argued that it was currently working to establish an enhanced 911 or E-911 system to replace call boxes in the city that would effectively allow those with disabilities to use public payphones to contact emergency services and provide an effective accommodation.[80] The court held that the city did not test the proposed tapping system on public payphones to the extent that it would be feasible for it to be used as an alternative, and therefore could not be used as a reasonable accommodation and allow removal of the emergency call boxes.[81] Under the ADA and Title II, a person with a disability does not have to have equal access to services as those who are not disabled, however the person must have "meaningful" access to publicly provided services.[82] A public entity should give primary consideration to individuals who are disabled when providing services to ensure that all citizens can access the same services.[83]

Judge Sweet determined that removing the boxes without providing an effective accessible alternative would violate Title II of the ADA by not providing a meaningful way for those with a disability to access the same emergency fire and police services as those without a disability, and the court prohibited their removal.[84] By forcing someone with a disability to rely on public payphones, which often do not work and are not located in as many places as

---

[79] CENTER FOR CONSTITUTIONAL RIGHTS, *supra* note 63.

[80] TRANSPORTATIONACCESS.COM, *supra* note 20.

[81] *Id.*

[82] *Civic Ass'n of the Deaf of New York City, Inc.*, 2011 WL 5995282, at *9.

[83] Hoffman, *supra* note 2.

[84] TRANSPORTATIONACCESS.COM, *supra* note 20.

emergency call boxes, the access to the public service is not meaningful and the accommodation is not sufficient.

Finally, the city argued that with the increased and widespread use of cell phones, alarm boxes are no longer needed as more individuals have personal phones that can be used to contact emergency services.[85] However, even if the public pay phones tell the dispatcher where the person is located, there is no way for someone who is deaf to indicate what type of service is needed and what the dispatcher should send for assistance.[86] Without being able to indicate what type of service is needed, a large risk occurs that the wrong service could be sent and a person with a disability could not be aided.[87] Judge Sweet refuted New York City's argument, stating that there was no system for either email or text message alternatives for those who are deaf or hard of hearing to contact emergency services at that time, which would have still prevented an individual with such a disability from being able to contact services without the emergency alarm boxes.[88]

V. Implications from Civic Association and Predictions

The most recent decision in Civic Association indicates that as technology progresses in the form of emergency communications, the need to protect those with disabilities and provide them access to emergency services will remain a constant. Beginning with the Rehabilitation Act Section 504 to the most recent ADA amendment in 2008, Congress and society have indicated that the need and desire to protect those with disabilities is a priority among the nation and when

[85] TRANSPORTATIONACCESS.COM, *supra* note 20.

[86] *Civic Ass'n of the Deaf of New York City, Inc.*, 2011 WL 5995282, at *4.

[87] *Id.*

[88] TRANSPORTATIONACCESS.COM, *supra* note 20.

creating law. Specifically, Civic Association indicates to major metropolitan areas, as well as any city within the United States, that if a public entity wishes to eliminate what they deem to be an outdated form of communication to implement a newer one, an accessible accommodation must be provided or the service cannot be removed. Those with disabilities are not asking for a greater service in refusing to allow the cities to eliminate older forms of emergency communications, rather those individuals are simply asking for equality in the form of emergency accommodations.

As society continues to develop and create new technologies that are faster and easier to use for emergency services, the problem will continue to arise as how to accommodate those with disabilities. It has taken a long period for the original emergency call boxes to become outdated due to cell phones, indicating that it might take some time for cell phones or payphones to become outdated with a newer technology. However, in recent years the rate at which technology has developed in both the public and private sectors has been astronomical compared to the mid and late twentieth centuries. NYC has already been working on a tapping system that they believe will be an effective means of communication for those with disabilities, a system that Judge Sweet recognized as a future possibility. This rapid development in emergency communication technology indicates that as newer methods are developed to accommodate all individuals, special attention will need to be given to individuals with disabilities to ensure their needs are protected and they can access emergency services.

In a recent age of financial insecurity, the desire for cities to eliminate costs by any means possible has become especially prevalent. Programs and services that were once deemed a necessity are now being phased out due to an inability to pay for them. This is what has occurred in NYC and what will most likely occur in the future as resources become even scarcer. Cities

will ultimately be forced with tough decisions like how to accommodate individuals with disabilities in emergency communications and how to afford these services. Instead of trying to identify how to accommodate two distinct groups of individuals, individuals with and without disabilities, it seems plausible that resources will be placed into stream lining communication and creating a system that is affordable and accessible to all individuals. In respect to affordability, it would seem appropriate that cities within the United States will unite to create a uniform system of emergency communication accessible to all individuals. A federal system for emergency communication that can be used by all individuals, regardless of disability, is a plausible and financially responsible means to achieve the goal of assisting people in times of emergency.

As the ADA continues to be affirmed, challenges of how to incorporate individuals with disabilities into the act will be present unless the ADA is amended to include a provision that accounts for changes in emergency communication systems. The issue of how to address those with disabilities using emergency communications is a forever-present issue. When the ADA is next considered for affirmation, Congress must add a clause to the act that specifically relates to this issue of emergency communications for the disabled. Adding a clause to the ADA that requires cities to automatically include accommodations for individuals with disabilities into new emergency communication systems will alleviate ADA lawsuits while providing access to more individuals. It would not be difficult to add a clause that would force public entities to provide adequate services for the disabled, while giving them the freedom to use new technologies to achieve the goal. If an amendment is not made to the ADA, then the gaps that are currently occurring between new technologies and ADA compliance will continue and leave individuals with disabilities unable to access emergency communications.

Finally, although not related to the legal issue of how to accommodate those with disabilities. It would seem appropriate that individuals with disabilities will become more involved in the process of how to better accommodate the disabled in the time of emergencies and the issue will be moved to the forefront of disability law. It is always difficult for a group to try and make changes to a law for another group without having adequate knowledge on the subject. Civic Association clearly indicated that NYC did not have the correct information or requisite knowledge when it tried to remove the emergency call boxes. If the city asked for input from the disability community, it would have known that the proposed idea was not a proper means to accommodate individuals with disabilities. Instead of the accommodations and legal standards being developed solely by those involved in the legal field, it would make sense that more activists and individuals from the disabled community to be involved in determining what should be done to ensure that as new technology is developed the ADA is complied with.

VI. Conclusion

There will always be a need in any industrialized nation for the government or some form of public entity to provide emergency communication services to those in need. The means by which the services are to be provided will change as time progresses, however, the need to assist all will remain a constant. Specifically, the need to protect those with disabilities and give them equal access to emergency services will remain a constant thanks to Congress and Federal Laws such as the Americans with Disabilities Act. Public entities will need to provide an efficient means for those with disabilities to receive assistance and ensure that the manner and style is not substantially different from the way those without disabilities receive assistance.

In a society that depends on technology and the "newer" and "faster" forms, public entities will struggle with creating cost effective systems that are on the forefront of technology while still providing access to all individuals. The Americans with Disabilities Act must be amended to ensure that as newer forms of emergency communications are produced individuals with disabilities will be accommodated. There is no errorless manner to dictate what will come from New York City or for the nation in creating emergency communication systems for the disabled, but with assistance from influential groups the system will survive and adapt to newer technologies.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 2, PAGE 26

The Quasi-Autonomous Car as an Assistive Device for Blind Drivers: Overcoming Liability and Regulatory Barriers

Dana M. Mele, J.D.

I. Introduction

The concept of a self-driving car is no longer the stuff of science fiction. From as early as the 1960s, engineers have worked on designs for autonomous vehicles.[1] However, in 2004, two challenges were extended that catapulted the race into hyper-drive. The Department of Defense ("DoD") Defense Advanced Research Projects Agency ("DARPA") issued the first DARPA Challenge, asking engineers to compete to create an autonomous vehicle that would contribute to research and development of autonomous vehicles for military purposes.[2] In the same year, the National Federation for the Blind ("NFB") announced a challenge to create another type of vehicle using cutting edge intelligent technology—a car designed for blind drivers.[3]

Google recently raised public interest, legal dispute, and safety concerns by developing a fleet of autonomous vehicles and, perhaps unsurprisingly, several other manufacturers now have

[1] John Markoff, *Google Cars Drive Themselves, in Traffic*, N.Y. TIMES, Oct. 9, 2010, *available at* http://www.nytimes.com/2010/10/10/science/10google.html?pagewanted=all.

[2] DARPA, *Grand Challenge '05*, *available at* http://archive.darpa.mil/grandchallenge05/overview.html (last visited Apr. 9, 2013).

[3] *About the Blind Driver Challenge*, NATIONAL FEDERATION OF THE BLIND, http://www.blinddriverchallenge.org/about-the-blind-driver-challenge (last visited Apr. 9, 2013).

driverless car prototypes in the works.[4] The vision of a former DARPA challenge runner-up, the Google car uses artificial intelligence to mimic decisions human drivers make.[5] Google argues that eliminating human decision from the equation will make roads safer.[6] After all, human error accounts for most of the 33,000 deaths and 1.2 million injuries on roads throughout the nation each year.[7] Google's autonomous vehicle program has already achieved 200,000 miles of computer-controlled driving without a single accident, and the company is already lobbying for state laws to permit driverless vans and taxis, hoping to achieve that reality by 2013 or 2014.[8] The major obstacle to achieving this goal is untangling major issues pertaining to liability.[9]

The NFB challenge raises questions of its own. In February 2011, Mark Riccobono, a blind executive of the NFB, drove a customized Ford Escape around a track filled with obstacles and another vehicle at Daytona International Speedway.[10] Dr. Dennis Hong, head of the team of engineers who designed and created the customized vehicle, estimates that with the technology,

---

[4] Sarah Jacobsson Purewal, *Nevada Approves Self-Driving Cars after Google Lobbying Push*, PCWORLD, Feb. 17, 2012, *available at* http://www.pcworld.com/article/250179/nevada_approves_selfdriving_cars_after_google_lobbying_push.html.

[5] Markoff, *supra* note 1.

[6] *Id.*

[7] John Markoff, *Collision in the Making Between Self-Driving Cars and How the World Works*, N.Y. TIMES, Jan. 23, 2012, *available at* http://www.nytimes.com/2012/01/24/technology/googles-autonomous-vehicles-draw-skepticism-at-legal-symposium.html (Google's vehicle has been involved in one accident but attributed the accident to human error, claiming that the accident occurred while the vehicle was in manual mode).

[8] *Id.*

[9] *Id.*

[10] Keith Barry, *High-Tech Car Allows the Blind to Drive*, WIRED.COM, Feb. 15, 2011, *available at* http://www.wired.com/autopia/2011/02/high-tech-car-allows-the-blind-to-drive/

blind drivers could be capable of travel on public roadways within five to ten years.[11] The car, designed for blind drivers, presents potential benefits for both blind and sighted individuals. It will contribute to goals of independence and autonomy for individuals with disabilities and provide valuable innovative technologies to increase safety for all drivers. Yet as with the Google fleet, technology is not the problem. The hindrance lies in questions of liability.

Despite potential benefits to blind and visually impaired as well as sighted individuals, however, barriers such as the potential liability to manufacturers and lack of a regulatory scheme may prevent this car from ever reaching the market. The vehicle is a new and likely a highly dangerous product with a substantial risk for manufacturer liability, and the lack of uncertainty regarding liability and marketing the vehicle without regulations in place will likely prove a large deterrence for manufacturers contemplating design and production. The potential for unpredictable and severe liability and an uncertain market due to lack of regulations for a product of this type may prove a fatal deterrence to manufacturers if no steps are taken to mitigate these barriers to production.

As with the fully autonomous car, determining liability for the "quasi-autonomous"[12] technology used in the car designed for blind drivers is difficult since its operation rests on the premise that the vehicle will deliver accurate information to the driver, and that the driver will use this information to make independent decisions. Because of the delicacy of this relationship, the line separating human error from robot error becomes razor thin, and determining liability is even more difficult than in the autonomous vehicle scenario. This note will discuss the issues of

[11] Barry, *supra* note 10.

[12] Although it is sometimes argued that all so-called autonomous vehicles are technically quasi- or semi-autonomous in a literal sense, I use the term "quasi-autonomous" throughout this note to distinguish vehicles that are operated by humans through interface technology rather than by computer decision-making technology.

liability and lack of regulation implicated by the quasi-autonomous car designed for blind drivers, why it is important that the liability and lack of regulation barriers be overcome, and how this might be accomplished.

Part Two of this note will briefly examine the evolution of the car designed for blind drivers and the technology it employs. Part Three will discuss the barriers to introducing this car to the marketplace, focusing on the problems presented by various liability theories and the challenges posed by manufacturing a vehicle without a dedicated regulatory scheme in place. Part Four will propose solutions to the problems discussed in Part Three, specifically, placing a limitation on applicable tort theories and creating a regulatory scheme for vehicles designed for blind drivers. The note will conclude with a proposed set of considerations for regulating licensure, ownership, and operation of these quasi-autonomous vehicles.

II. Inception of the Blind Driver Challenge and the Evolving Quasi-Autonomous Vehicle

The car designed specifically for blind drivers has long been in the works. The technology required to realize the original conception, once begun, has evolved rapidly. Unfortunately, the introduction of this car onto the public roadways may be a much longer journey. This section will proceed by briefly introducing the history and objectives of the NFB Blind Driver Challenge. It will then examine the evolution of the technology used in the development of the vehicle and designed in response to the challenge, which will be used for the purposes of this note as a prototype for cars designed for blind drivers using similar interface technologies. The section will conclude with a brief look at future uses of the technologies utilized in the vehicle.

A. Development of a Car for Blind Drivers

The concept of a car that can be driven by blind drivers is hardly novel. Dr. Mark Maurer, president of the NFB, had spoken publicly about the possibility of developing such a vehicle for years prior to the inception of the Blind Driver Challenge.[13] On January 30, 2004, however, the NFB Jernigan Institute, the first research center created and run by blind individuals, was opened, and the Blind Driver Challenge ("BDC") was extended.[14] The BDC offered a challenge to universities and developers of innovative technology to formulate and build an interface technology that would allow blind people to drive a car.[15] The essence of the challenge is to develop technology that is not fully autonomous, giving a blind individual the role of a passenger while the car drives itself, but instead a non-visual interface that permits a blind individual to assume the role of driver using essentially assistive technology to inform the driver about driving conditions.[16]

The reason the NFB emphasizes non-visual interface technology instead of pure autonomous technology is reflected in the stated purposes of the BDC. The first objective is to advance non-visual access technology and to close the gap between access technology and technology in general.[17] Solely autonomous vehicles relegate blind individuals to the role of a passenger. This fails to advance technology that will enhance non-visual access and further widens the gap between the technology used to drive for sighted and blind drivers. If technology

[13] *About the Blind Driver Challenge*, *supra* note 3.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] National Federation of the Blind, NFB Blind Driver Challenge, https://nfb.org/nfb-blind-driver-challenge (last visited Apr. 9, 2013).

for blind drivers is limited to fully autonomous vehicles, it will perpetuate an active/passive distinction between sighted and blind drivers.

The second objective is to increase awareness in the scientific community about barriers facing blind individuals.[18] The challenge itself serves this objective, but purely autonomous vehicle technology runs the risk of minimizing the barriers blind individuals face because fully autonomous technology simply does not address these barriers. While a purely autonomous vehicle mimics human decision-making functions,[19] interface technology highlights the numerous pieces of typically visually presented information that drivers must gather in order to make driving decisions. The interface technology reinforces the existence of these barriers for blind individuals, while fully autonomous vehicles gloss over the barriers by gathering the data, processing it, and eliminating the human element.

The third objective is to solve problems facing blind and sighted individuals and create new opportunities and paths to success through the use of non-visual technology.[20] This goal encourages non-visual technologies that will benefit both blind and sighted individuals and will help to move innovation toward design that is universally accessible for people with and without visual impairments. Fully autonomous vehicles arguably meet the objective of contributing a universally accessible design, but again, the universal application is limited to providing a new passive role for both blind and sighted individuals, whereas the rest of the objectives favor an active role for blind individuals.

The fourth and final objective of the BDC is to alter public perception of blind individuals by demonstrating the ability to drive using assistive technology, and to show blind

[18] National Federation of the Blind, *supra* note 17.

[19] Markoff, *supra* note 1.

[20] National Federation of the Blind, *supra* note 17.

individuals as people with ambition for greater independence.[21] Here, fully autonomous vehicles would fail most markedly. Assigning blind individuals a passive role severely undermines the goal of demonstrating the ability to drive with assistive technology. In addition, while fully autonomous vehicles will increase independence in some measure by allowing greater transportation freedom, it will not empower the individuals to interact with the technology and participate in the process. The individual will still be a passenger and not a driver.

The history of the BDC shows remarkable progress in the pursuit of these goals. As mentioned above, the idea of a car for blind drivers was formulated far before the BDC was initiated. The NFB first began raising money for the Jernigan institute in 1999, at which time Dr. Maurer announced that one of the Institute's projects would be the development of such a vehicle.[22] At the groundbreaking of the Institute in 2001, Dr. Maurer stated that researchers who create products to increase access for blind individuals to information, to transportation, and to the business community would form an important component of the Institute's mission.[23] At the grand opening of the Institute in 2004, the NFB showcased a mock-up of a vehicle for blind drivers and announced the challenge for the first time.[24] In 2005, the NFB invited all American

[21] National Federation of the Blind, *supra* note 17.

[22] Mark A. Riccobono, *Driving Independence and Innovation through Imagination: The NFB Blind Driver Challenge*, BRAILLE MONITOR, Dec. 2009, *available at* http://www.nfb.org/images/nfb/Publications/bm/bm09/bm0911/bm091103.htm (last visited Apr. 9, 2013).

[23] *Id.*

[24] *Id.*

universities to take up the challenge, and in 2006, Virginia Tech was the only school, or invitee, to accept.[25]

Virginia Tech's Dr. Dennis Hong and his group of undergraduate students at Robotics and Mechanisms Laboratory ("RoMeLa") designed their first vehicle in the 2008-2009 school year.[26] In May 2009, Wes Majerus and Mark Riccobono, of the Jernigan Institute, were the first completely blind from birth people to drive the original model through an obstacle course of traffic cones.[27] In the summer of 2009, Virginia Tech's BDC team participated in the NFB Youth Slam, in which blind students tested the team's first model.[28]

The goal of the current BDC challenge as of 2011 is to not only put a vehicle on the road, but to have blind individuals drive it from the NFB Jernigan Institute to the NFB National Convention.[29] To meet these objectives, the technology, first formulated in 2008, has had to make enormous progress in little time.

B. The Technology of the RoMeLa Car

As the goals of the BDC have progressed, the technology employed to meet those goals has likewise advanced. The Virginia Tech team chose to meet the BDC challenge by starting

[25] *Blind Driver Challenge History*, VIRGINIA TECH ROBOTICS MECHANISMS LABORATORIES (NOV. 10, 2010), available *at* http://www.romela.org/blinddriver/BDC_History (Apr. 9, 2013) [hereinafter *Blind Driver Challenge History*].

[26] *Id.*

[27] *Id.*

[28] Riccobono, *supra* note 22.

[29] *Id.*

with an existing platform, and developing non-visual driver interfaces to allow blind individuals to drive the integrated vehicle.[30]

Virginia Tech's original 2008-2009 design team chose a stock dune buggy as the platform for the first attempt.[31] The team aspired to create a vehicle that would maximize both independence and safety by allowing a blind driver to navigate and drive through a traffic cone course.[32] This original design relied on a Hokuyo single plane laser range finder sensor ("LRF") to gather information about obstacles surrounding the vehicle.[33] The team then created a "click wheel" to convey the information to the driver by delivering audio cues in the form of "clicks" for each measured "turning unit."[34] The driver would respond to the cues by turning the wheel accordingly and altering the direction of the vehicle.[35] Finally, the team designed a vest to deliver tactile information about speed to let the driver know when to decelerate the vehicle or to initiate an emergency stop.[36] Vibrating motors inside the vest line both sides of the driver's chest and are programmed to vibrate on the right side if the speed limit set by the program is exceeded by the driver, and to vibrate on both sides if an emergency stop is required.[37] The test

[30] *Blind Driver Challenge History*, *supra* note 25.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Blind Driver Challenge History*, *supra* note 25.

[35] *Id.*

[36] *Id.*

[37] *Id.*

drives of this original vehicle were successful. However, the vehicle itself vibrated excessively, a feature the team chose to work on in its next design.[38]

The Senior Design Team at Virginia Tech's RoMeLa labs found that the vibrations in the 2008-2009 design interfered with the operation of the interface technology, so they chose a new platform, a golf cart, as the basis for the 2009-2010 vehicle.[39] This new platform was chosen primarily in order to solve the problem of the interference caused by vibrations, and because of the additional advantage of a quiet engine.[40] The 2009-2010 team also decided to replace the click wheel system with a new tactile information system, "DriveGrip."[41] DriveGrip uses vibrations on the hands to deliver turning information, such as when to turn, where to turn, and how far to turn.[42] The team also chose to redesign the tactile vest in order to make it adaptable to more platforms, and the end product was a tactile shoe.[43] In addition to information about deceleration and emergency stopping, the tactile shoe delivers information about accelerating and braking through vibration along the top and bottom of the shoe.[44]

The 2010-2011 design team again broadened its vision by selecting a TORC ByWire XGV as its platform.[45] The ByWire XGV, discussed below, is a modified drive-by-wire Ford

[38] *Blind Driver Challenge History*, *supra* note 25.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Blind Driver Challenge History*, *supra* note 25.

[43] *Id.*

[44] *Id.*

[45] *Id.*

Escape Hybrid developed to test unmanned vehicle technologies.[46] In addition to using an actual car for its platform, the 2010-2011 senior design team worked to improve the DriveGrip technology and to develop SpeedStrip, an innovative interface that communicates to the driver when to accelerate, decelerate, and stop.[47] SpeedStrip delivers the information to the driver by means of vibrations in the back and the bottom of the driver seat.[48] The driver then decides the amount of pressure to apply to the brakes based upon the strength of the SpeedStrip vibrations.[49] Installed on a TORC ByWire XGV, the 2010-2011 goal of this design was to empower the driver with more independence to make decisions and to enhance maneuverability, allowing the car to take part in the Rolex 24 GRAND-AM road race at Daytona International Speedway.[50]

In June of 2010, Virginia Tech's RoMeLa joined forces with TORC, a developer and manufacturer of modular unmanned vehicle technologies, to create the 2010-2011 BDC design.[51] RoMeLa's Dr. Hong announced that the design team chose TORC's ByWire XGV because of its performance, compatibility with RoMeLa's design system, and record of reliability in order to prioritize safety.[52]

TORC's ByWire XGV is a modified Ford Escape Hybrid with drive-by-wire conversion modules, which is a "thoroughly tested" basic platform onto which innovative technologies can

[46] *Blind Driver Challenge History*, *supra* note 25.

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Blind Driver Challenge History*, *supra* note 25.

[51] TORC Robotics, *NFB Blind Driver Challenge Team Chooses TORC's ByWire XGV as Base Research Platform*, Press Release, Oct. 13, 2010, *available at* http://www.torctech.com/media/press-release/nfb-blind-driver-challenge-team-chooses-torcs-bywire-xgv-base-research-platform/ [hereinafter TORC Robotics Press Release].

[52] *Id.*

be integrated.[53] The Drive-by-Wire Ground Vehicle Platform, from TORC's Robotic Building Blocks line of products, is a robotic system controlled by a computer.[54] This system allows all functions required to drive the vehicle safely, including the throttle, brakes, steering, engine, fuel levels, lights, signals, horn, and wheel speeds.[55]

The XGV modified Ford Escape Hybrid also features a PowerHub power distribution module.[56] The TORC PowerHub is designed to distribute power throughout unmanned systems by computer control, and may be controlled remotely.[57] Finally, the XGV is equipped with TORC's SafeStop wireless emergency stop system.[58] The SafeStop system was developed to allow unmanned vehicles to be paused or stopped by remote control by disabling the operation of the vehicle completely.[59]

As its next step, the RoMeLa team has chosen to prioritize developing technology to maximize driver safety.[60] In order to achieve this goal, the team will focus on the three primary

[53] TORC Robotics Press Release, *supra* note 51.

[54] TORC, Robotic Building Blocks, http://www.torcrobotics.com/robotic-building-blocks (last visited Apr. 9, 2013).

[55] *Id.*

[56] TORC Robotics Press Release, *supra* note 51.

[57] TORC, PowerHub Power Distribution Module for Robotic Systems, http://www.torcrobotics.com/products/powerhub-power-distribution-module-robotic-systems (last visited Apr. 9, 2013).

[58] TORC Robotics Press Release, *supra* note 51.

[59] TORC, SafeStop Wireless Emergency Stop System for Unmanned Vehicles, http://www.torcrobotics.com/products/safestop-wireless-emergency-stop-system-unmanned-vehicles (last visited Apr. 9, 2013).

[60] Virginia Tech Robotics Mechanisms Laboratories, Blind Driver Challenge Future, http://www.romela.org/blinddriver/BDC_Future (last visited Apr. 9, 2013).

hardware components of the system.[61] These components are the sensors, the audio and steering angle interfaces, and the tactile vest.[62] The team also plans to work on the software system in order to improve the way collected data is processed so that it can be more easily synthesized and delivered via the interface system.[63] In addition to fine-tuning the current DriveGrip and SpeedStrip technologies to deliver information about speed adjustments and timing and degree of turns, the team will work on a new technology, AirPix.[64] AirPix will use a system of compressed air pushed through small holes in patterns, similar to an air hockey table.[65] AirPix will create a "tactile image" that a driver can access by holding his or her hand over and feeling the pattern as if a picture of the environment were projected against it.[66] Perhaps the greatest improvement of this system is that it maximizes the potential for blind drivers to make independent decisions based on their own judgment using the information about the environment provided by the technology.

The current state of the car uses all of these technologies to allow the most independence on the part of the driver. On Jan. 29, 2011, Mark Riccobono drove the XGV model around the inner track of the Daytona International Speedway at 25 miles per hour, navigating around obstacles and another vehicle.[67] According to Jesse Hurdus, a TORC software engineer, the vehicle used at that time "replicated the eyes of a human and the parts of the human brain and

[61] Virginia Tech Robotics Mechanisms Laboratories, Blind Driver Challenge Future, http://www.romela.org/blinddriver/BDC_Future (last visited Apr. 9, 2013).

[62] *Id.*

[63] *Id.*

[64] Barry, *supra* note 10.

[65] *Id.*

[66] *Id.*

[67] *Id.*

nervous system" used for driving with hardware, software, and sensors.[68] In addition to the equipment described above, the car used a GPS system, cameras and laser scanners, and an "Inertial Measurement Unit" to replicate the functions of the inner ear.[69] The team plans on making future improvements, however.

The goal for the future of RoMeLa's BDC is to meet the initiative's ultimate challenge: to develop and build a workable vehicle that a blind person can drive independently.[70] Dr. Hong predicts that blind drivers could potentially travel on public roadways within the next five to ten years.[71] However, in keeping with the challenge's goal of increasing independence for blind people and using non-visual interface technology for both blind and sighted people, future uses of the technology developed for the BDC encompass wide-ranging possibilities outside of assisting blind people to drive independently.

C. Future Uses

Scientists predict that the technologies may be used to enhance the use of appliances, offices, and schools.[72] For example, the AirPix technology currently being developed by RoMeLa and other non-visual interfaces developed by the lab for the BDC may be developed for

[68] Barry, *supra* note 10.

[69] *Id.*

[70] Work Continues to Advance, Adapt Blind Driver Technology, http://www.vt.edu/spotlight/impact/2011-02-28-bdc/daytona-side.html (last visited Apr. 9, 2013).

[71] Barry, *supra* note 10.

[72] *Id.*

classroom use, so that when a teacher writes on a blackboard, blind students will be able to access the information through the interfaces and read what the teacher writes.[73]

Sighted individuals will also benefit from the technology. The interface technology can enhance a sighted person's ability to drive in heavy fog, for example, or in the dark, where vision is impaired by environmental factors.[74] The laser-range finder technology used to create a warning alarm system for dangerous conditions will benefit sighted as well as blind drivers.[75] In addition, existing technology to prevent lane departure and active cruise control can potentially be enhanced by these new innovative interface technologies.[76] Although these benefits are wide reaching and universally applicable, however, the threat of liability may prevent them from reaching the public.

III. Barriers to Production: Liability and Lack of Regulation

A car developed for blind drivers faces serious barriers, despite the rapidly developing technology and the vast potential benefits and uses. The potential liability of the manufacturer of the prospective car that may be developed and marketed for blind drivers is a key factor, since questions of liability may influence the zeal with which this goal is pursued, and a high risk of liability may have a chilling effect on innovation.[77] M. Ryan Calo, a fellow at the Stanford Law School's Center for Internet and Society and Co-Chair of the Artificial Intelligence and Robotics

[73] Barry, *supra* note 10.

[74] *Id.*

[75] Work Continues to Advance, Adapt Blind Driver Technology, *supra* note 70.

[76] Barry, *supra* note 10.

[77] *See* Richard Acello, *Robot Rules Lawyers Ponder Liability for Actions by "Thinking" Machines*, ABA J., May 2010, at 29.

Committee of the ABA, cautions that the uncertainty about liability in the field of robotics could discourage innovation and cause the United States to fall behind other countries in a vital area of technological development.[78] Lack of provisions in vehicle regulatory schemes to provide for blind drivers and cars developed for blind drivers with built-in assistive technologies are also a major barrier to allowing the car a pathway to the marketplace, since the manufacturers have no incentive to make the car if regulations prohibit its use. The sections below will discuss the problems posed to manufacturers by negligence and strict products liability theories and by a lack of applicable regulatory provisions.

A. Barriers Posed by Potential Liability Theories

First, it is difficult to determine liability in computer and robotic products. Since this car encompasses both, this signals a potential problem for manufacturers. Courts are generally unwilling to impose liability for injury caused by computer unless the injury is physical and is caused by computers or software, usually where a medical or navigational malfunction results in physical injury.[79] This is a potentially foreseeable problem for a car equipped with hardware and software to facilitate navigation by supplying a blind driver with navigational and environmental data.

[78] M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 576 (2011).

[79] *Id.*

B. Problems Posed by Applying a Negligence Theory

Various experts have suggested applying negligence theories in cases involving computer software and hardware.[80] This could have both positive and negative consequences from a public policy standpoint. On one hand, developers of software and computer systems, if exposed to greater liability, will have a greater incentive to create safer products, and are in the best position to prevent harmful security breaches in the first place.[81] On the other hand, as discussed in this note, too much exposure to liability will deter manufacturers from placing the product on the market in the first place.

In order to succeed in a negligence claim, an injured plaintiff must prove that the defendant owed her a duty of care, that the defendant breached the duty of care, that such breach was the proximate and factual cause of the plaintiff's injury, and that the plaintiff suffered a compensable injury resulting from the breach of duty.[82] Applied to an accident resulting from a scenario in which a blind driver makes a decision based upon faulty information due to a software error, and causing physical injury, the following problems may arise.

First, the plaintiff driver bringing a claim against the manufacturer of the car must establish that the manufacturer owed her a duty of care.[83] Regarding the software, the manufacturer may owe a duty to design and develop secure software that is not defective, and a

[80] Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 441 (2008).

[81] *Id.* at 442.

[82] *Id.*

[83] *See* RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 6 (2010) (Comment B discussing the elements of liability for physical harm caused by negligence). [Hereinafter Elements of Negligence].

duty to inform the driver of hidden dangers, as well as how to use the car safely.[84] The duty of software manufacturers would likely include an assessment of the foreseeability of harm caused by a malfunction.[85] In this case, the foreseeability of a malfunction of the software may be considered high because the technology is new and untested. The degree of certainty between the vulnerability of the software and harm is also an important consideration.[86] Again, the degree is likely high, because the purpose of the product is for drivers who would not otherwise be able to drive safely to rely on the software and other technological features of the car to make informed decisions in order to perform the task of driving safely. Without secure software, the product is inherently and highly dangerous to the user and to others. Because the driver relies on the information these technologies provide, the degree of danger inherent in the product is not analogous to the danger of a blind driver using a car with typical features, and the duty owed is higher than that of a manufacturer of a car that does not offer these features and market itself as a car for blind drivers. It is a specialized vehicle that would be inherently dangerous regardless of degree of impairment or lack thereof because the purpose of the product is to rely on the software and robotic features. Therefore, the duty of care should be very high, creating one substantial obstacle for manufacturers.

As far as breach of duty,[87] experts in the field of computer liability urge that vendors of software should be found negligent if they market products when there is a high foreseeability of

[84] Scott, *supra* note 80, at 443.

[85] *Id.* (positing that the determination of duty is largely policy-based and will require courts to consider the foreseeability of malfunction or security breach in the case of software liability, *quoting* Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 519-20 (2006) for the latter proposition).

[86] *Id.*

[87] *See* Elements of Negligence, *supra* note 83.

harm and "readily available means 'to eliminate or reduce the risk of harm.'"[88] By this standard, there may be a high foreseeability of harm because of the arguably inherently dangerous nature of the product. This creates a second potential problem for the manufacturer, but only if the plaintiff can prove that there are readily available means to eliminate or reduce the risk of harm.

As for factual cause,[89] it will be difficult to prove that "but for" the defect, the injury would not have occurred since the car is designed to maximize the driver's independence and decision-making ability through interface technology, unlike the self-driving cars being developed by Google and designed by other manufacturers. However, the plaintiff may also show that the alleged negligence was a substantial factor in causing the injury,[90] and the plaintiff injured by either a design or warning defect in a ByWire XGV type car for blind drivers may have little trouble demonstrating that this defect was a substantial factor in causing the injury.

In order for the plaintiff to prove proximate cause,[91] she will have to prove that the injury was a foreseeable result of the negligence.[92] In a case often cited in software liability discussions, the U.S. Court of Appeals for the Second Circuit held that where a manufacturer of navigational charts supplied faulty information in its charts leading to a fatal plane crash, the provision of the incorrect data was the proximate cause of the injury and the defendant manufacturer was liable.[93]

---

[88] Scott, *supra* note 80, at 443.

[89] *See* Elements of Negligence, *supra* note 83.

[90] Scott, *supra* note 80, at 443.

[91] *See* Elements of Negligence, *supra* note 83.

[92] Scott, *supra* note 80, at 443.

[93] Saloomey v. Jeppesen & Co., 707 F.2d 671, 677 (2d Cir. 1983) (holding that even though the court below found that the pilot and air traffic controller were also negligent, the manufacturer's negligence in the manufacturing and inspection of the navigational charts was the proximate cause of the injury); *See also* Brocklesby v. United States, 767 F.2d 1288, 1297 (9th Cir. 1985) (upholding a jury verdict on the

Professor Michael Scott, author of seven legal treatises on information technology law, distinguishes *Saloomey v. Jeppesen & Co.*, from software security cases because it involves an easily identifiable negligent act, whereas security breaches in software are difficult to identify.[94] However, in the case of a driver relying on interface technologies, as in *Saloomey*, the primary negligent act is providing faulty information, upon which the use must rely in order to safely and properly operate the vehicle. If courts analyze the hypothetical presented as analogous to *Saloomey* as is often suggested for software liability cases resulting in physical injury, there is a high likelihood that the plaintiff can prove proximate cause.

Taken together, there is a chance that on a negligence theory, a plaintiff will be able to prevail against a manufacturer of a car designed for blind drivers, creating a barrier for production and marketing. However, further and likely more serious barriers exist under strict products liability theories.

C. Problems Posed by Applying a Strict Products Liability Theory

If a negligence theory poses risks to the manufacturer, a strict liability theory presents a potentially larger threat. Under a design defect, warning defect, or manufacturing defect, public policies would be served but the risks to the manufacturer would be so high that the possibility of barring the product from reaching the marketplace is a crucial consideration.

---

grounds that Jeppesen, the same manufacturer, was negligent for failing to warn consumers of latent defects in a navigational chart resulting in an airplane crash that killed 6 crew members).

[94] Scott, *supra* note 80, at 449.

For example, there is a design defect where a foreseeable risk of harm could have been avoided or reduced by the use of a reasonable alternative design ("RAD").[95] In the case of the vehicle designed for blind drivers, there is currently and will likely at first be no RAD. But a RAD could easily and at any time be developed, placing the manufacturer in a vulnerable position when the product is at the point of inception and rapid innovation is crucial in order to ensure both that the product becomes available and that technology continues to evolve to create a safer and more efficient product.

Under a manufacturing defect analysis, manufacturers may be liable even if their safety standards are reasonable. A product has a manufacturing defect when it "departs from its intended design even though all possible care was exercised in the preparation and marketing of the product."[96] This presents a particularly serious danger to manufacturers of new products that have the potential to cause serious physical injury. In this case, a car that requires the manufacturing of novel and previously untried hardware and software that must operate flawlessly in order to avoid a very high risk of serious physical injury is a dangerous gamble.

Finally, under a warning defect claim, a manufacturer may be held strictly liable if a product is defective due to inadequate warnings or instructions and foreseeable risks of harm could have been reduced or avoided by reasonable alternative instructions or warnings.[97] Again, although like a design defect, this theory allows for a consideration of reasonableness, because the product is new. The strict liability theory creates high stakes for the manufacturer, and a

[95] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).

[96] *Id.*

[97] *Id.*

"reasonable alternative" creates more danger than it avoids because the competition is largely unknown and will likely spring up suddenly and develop rapidly.

D. Breach of Warranty under Article 2 of the Uniform Commercial Code

One final possible theory of liability is breach of warranty under Article 2 of the Uniform Commercial Code ("U.C.C.").[98] Software dedicated to a particular use and bundled with a tangible product generally falls under Article 2 of the U.C.C. and allows vendors to shield themselves from liability by using warranty disclaimers and by limiting liability and remedies.[99] This description may apply to the ByWire XGV since it depends on software. Both express and implied warranties can be disclaimed by contract and are usually presumed to be valid. However, warranty disclaimers are construed strictly in the favor of the purchaser.[100] Nonetheless, no court to date has held a software vendor in violation of an express warranty, and courts have usually upheld implied disclaimers of warranty only if the warranty is not unconscionable and if there is privity of contract between the parties.[101] In addition, courts have split on the question of whether each party in a chain of distribution must disclaim warranty in order for the disclaimer to be effective.[102] In the case of a car, which often has several steps in the chain of distribution, this leaves much leeway. Nonetheless, under Article 2, whether through warranty disclaimers,

---

[98] *See* U.C.C. § 2-312(1)(a) (implied warranty of title); § 2-313(1)(a) (express warranties); § 2-314 (implied warranty of merchantability); § 2-315 (implied warranty of fitness for a particular purpose).

[99] Scott, *supra* note 80, at 435-37.

[100] *Id.* at 437.

[101] *Id.* at 439.

[102] *Id.* at 438-39.

limited liabilities, or limited remedies, manufacturers are shielded from liability and therefore given a greater opportunity for innovation without fear of legal responsibility. However, because of the dangerous nature of the car, the software package and the manufacturer may be exposed to more liability.

E. Barriers Posed by Lack of Regulation

A second difficulty in the movement toward placing the car designed for blind drivers on the market is a lack of regulation. In general there is little regulation in the field of autonomous technology, so it is minimally helpful to look to this area as far as formulating regulations. Professor Susan Brenner argues that pervasive technologies – technologies intended to be used by all, and not merely by specialists that have a pervasive effect – presents difficulties for the law, although consumer technologies, which she calls modestly pervasive, have traditionally allowed for a set of rules based on a non-pervasive system.[103] However, Professor Brenner posits that this is based on the fact that most consumer technologies have limited potential for misuse.[104] Professor Brenner categorizes both automobiles and computers as pervasive and consumer technologies.[105] According to Professor Brenner, the problem with these rules is that they are based on problems of defective implementation, which relies on expert use, and not proper implementation; however, she points out that in the case of automobiles, society has successfully created rules to regulate "civilian" use.[106] The integration of automobile use - predicated already

[103] Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 671-72 (2006).

[104] *Id.* at 671.

[105] *Id.* at 708-10; 733-34.

[106] *Id.* at 763.

on human control of a product that must not be defective - with software, which is loosely regulated, is the dilemma for those contemplating regulatory schemes for a car designed for blind drivers.

The operation of motor vehicles is regulated. Since 1908, states have required drivers to pass mandatory tests and possess various eligibility qualifications in order to earn a license to drive.[107] So-called new technology, including software, however, is very lightly regulated. For example, government agencies have not yet implemented regulations to control the use of products containing nanotechnology.[108] In the context of software manufacturer liability, there are no established regulations that govern "the performance of software programmers and developers."[109] M. Ryan Calo writes that technology policy is currently shaped by concerns about the optimal conditions for innovation and competition.[110] He writes further, however, that in the context of robots, government regulation could make products safer.[111] This suggests strongly that the stringency of the regulation and the freedom to innovate, or such perceived freedom, are in tension.

IV. Overcoming the Barriers to Production

In spite of the obstacles facing policymakers and lawmakers in devising schemes to regulate and create liability frameworks for vehicles with autonomous vehicles designed and

[107] Brenner, *supra* note 103, at 712.

[108] Shalyn Morrison, *The Unmanned Voyage: An Examination of Nanorobotic Liability*, 18 ALB. L.J. SCI. & TECH. 229, 245 (2008).

[109] Scott, *supra* note 80, at 472.

[110] Calo, *supra* note 78, at 578.

[111] *Id.* at 604.

marketed for blind drivers, there are some solutions. One of the biggest concerns in both imposing liability and regulation has been the danger of the chilling effect potential liability may have on valuable innovations. Despite these concerns, the car and the technologies it employs present great benefits to blind and sighted individuals, to the disability community, and to the general public. They contribute important innovations that can be utilized in a variety of products to enhance safety, efficiency, and convenience in numerous contexts. On balance, the benefits of striving to place a car for the blind on the market outweigh the difficulties that must be overcome in order to do some. This section will detail some of the benefits and uses of the car and other applications of the technology it uses, propose a solution to the liability concerns that create a barrier for manufacturers, and discuss possible regulatory regimes for quasi-autonomous cars designed for and driven by blind drivers.

A. Benefits of Overcoming the Barriers

Having a quasi-autonomous car for blind drivers on the market will benefit blind and sighted individuals. The original objectives of the Blind Driver Challenge were to "close the gap" between access technology and general technology, to increase awareness in the scientific community about barriers facing blind individuals, to solve problems facing blind and sighted individuals and encourage technology that is universally accessible to all, and to alter the public perception of the blind by demonstrating the ability to drive using assistive technology.[112] These objectives, and the car RoMeLa labs has created and continues to perfect, are consistent with objectives of federal disability law, which advance independence and accessibility of individuals with disabilities as a paramount national concern. I argue that access to driving, as a means of

[112] Riccobono, *supra* note 22.

independent travel, is among those concerns, and that current disability law supports this contention.

Although the Americans with Disabilities Act of 1990 and the ADA Amendments Act of 2008 (together "ADA") do not allow a general right to accessible roads or highways, or a right to travel on state controlled highways, the findings and purpose of the ADA are consistent with promoting independence and assistive technology as a means to achieve that end.[113] The Department of Transportation ("DOT") contains some general provisions that may provide some guidance for lawmakers wishing to craft regulations or further define travel accessibility under the ADA.[114] The regulations also include a general non-discrimination clause, which provides that "[n]o entity shall discriminate against an individual with a disability in connection with the provision of transportation service."[115]

The Rehabilitation Act of 1973 also supports the development of a car for blind drivers in its general purpose. Section 504 contains a general non-discrimination provision which states that "[n]o otherwise qualified individual with a disability in the United States, as defined in section 705(20) of this title, shall, solely by reason of her or his disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance or under any program or activity conducted by any Executive agency or by the United States Postal Service."[116] While the ADA covers state programs, such as Departments of Motor Vehicles, the Rehabilitation Act covers programs ad

[113] *See* Americans With Disabilities Act of 1990, 42 U.S.C. § 12101 et seq. (2006).

[114] *See* 49 C.F.R. §37 Subpart A (2011).

[115] *Id.* at § 37.5(a).

[116] 29 U.S.C. § 794 (2006).

activities that accept federal funding as well as Executive agencies. The DOT, for example, has issued requirements for federal highways.

The DOT regulations provide that discrimination by an entity that receives federal funding is prohibited on the basis of disability.[117] Discrimination includes denying a person with a disability the opportunity to participate or benefit from an aid, benefit, or service, that the opportunity must be substantially equal to that afforded a person without a disability, and must be as effective in affording equal opportunity "to obtain the same result, to gain the same benefit, or to reach the same level of achievement" as persons without disabilities.[118] The federal highways are regulated, in that highway rest area facilities, curb cuts, and pedestrian over-passes, under-passes and ramps must conform to accessibility standards.[119] Although the DOT has chosen to regulate only small portions of the highways, it suggests that the government has an interest in increasing accessibility in travel on federal highways for drivers with disabilities. Although the government has thus far declined to extend the regulations so far, the manufacturing of these cars provides an incentive and important reason to do so.

Furthermore, the recent Federal Highway Administration's (FHWA) Americans with Disabilities Act (ADA) Program has extended access for individuals with disabilities, although it has not gone so far as to cover highway travel by automobile. Still, taking the sum of these laws together, the spirit and intent, along with the trend of expansion and the underlying goal of increasing independence, suggests that major federal disability laws support the entry of a quasi-autonomous car for blind drivers onto the market, as well as the introduction of drivers who are blind and have visual impairments into the group of automobile consumers and highway drivers.

[117] 49 C.F.R. § 27.7 (2011).

[118] *Id.* at § 27.7(b)(1)(i)-(iii).

[119] *Id.* at § 27.75 (2011).

In addition, the Assistive Technology Act of 2004[120] ("ATA") supports the conclusion that the car designed for blind drivers might be considered assistive technology. First of all, giving blind Americans the opportunity to drive is consistent with the findings and purposes of the ATA. The ATA promotes independence, participation, self-determination, the ability to pursue and successfully carry out a career, and generally promotes the objectives of inclusion and integration, also major objectives of the NFB Blind Driver Challenge.

Under the ATA, a vehicle can be an assistive technology device. The ATA defines an assistive technology device as "any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities."[121] This vehicle falls well within this definition, and the individual features qualify as well as modifications.

The ATA may also provide an avenue for funding, an obstacle that stands in the way of getting the car designed for blind drivers from design to reality. The ATA provides for grants to states to maintain "comprehensive statewide programs of technology-related assistance" for programs that increase access to assistive technology and maximize the ability of individuals with disabilities to obtain assistive technology.[122] Such funding could be applied to state programs designed to help blind individuals obtain training, licensure, insurance, and other requirements for driving. Programs could be established with this funding, or other state grants in a similar spirit, to provide driver's education taught by and for blind individuals for the purpose of driving the specialized quasi-autonomous cars under the regulations to be prescribed

[120] Assistive Technology Act of 1998, 29 U.S.C. § 3001 (2006).

[121] 29 U.S.C. § 3002(4) (2006).

[122] *Id.* at § 3003(e).

by state authorities. Under this provision of the ATA, funding could also go toward a voucher program to help individuals gain access to rental cars since it facilitates access to assistive technology that fosters independence.

In addition to the important role the car for blind drivers would play in the disability field, the technology would enhance safety in driving. While completely autonomous vehicles promise a safer car because car accidents are nearly always attributable to human error, the figures that support this conclusion fail to take into account that human calculation is able to avoid collisions that computers cannot. For example, a fully autonomous car would not be able to interact with other human signals, such as a safety worker signaling the car to stop or pass, and even when the cars have been developed to match human capabilities they may not be able to interact appropriately with human drivers—for example when human drivers bend rules by rolling through stops or break traffic rules.[123]

In contrast, the interface technology of the quasi-autonomous car is designed precisely to present accurate information to enhance, not compete with, human decision-making. Because the car is designed with such a purpose in mind, the technology would aim to provide non-visual information about the safety worker's signals in the example above, or the environmental factors, including obstacles like other cars. During the 2011 test drive of RoMeLa's ByWire XGV, Riccobono navigated the car around obstacles and passed another car on the same path while maintaining completely control. The car is designed to promote driver autonomy. Universal benefits for blind and sighted drivers include application of the technologies to low vision environments, such as dark or foggy driving conditions.[124] However, because the risk of liability

[123] Markoff, *supra* note 7.

[124] Barry, *supra* note 10.

and lack of regulations in place threaten to prevent the car from reaching the marketplace, steps must be taken to minimize liability and put regulations in place.

B. Liability Should Be Limited to Negligence

Placing limits on manufacturer liability will mitigate the deterrence problem. If the exposure to liability is reduced, manufacturers will have incentive to pursue further development of the quasi-autonomous car for blind drivers, and the benefits of having such a car available will provide advantages to the general public as well as to blind drivers. Specifically, limiting liability to negligence and eliminating a strict liability theory will encourage innovation and the end result will benefit consumers and serve to increase independence for blind individuals.

As discussed above, strict liability theories pose substantial threats to manufacturers because of the low burden placed on plaintiffs. Under a manufacturing defect claim, a plaintiff need not show that the manufacturer acted unreasonable. Under a warning or design defect a plaintiff need only show that a reasonable alternative existed that would have reduced or eliminated the risk of injury, an obstacle too easy to overcome in this instance. Because the product is so new, as discussed above, the possibility of a reasonable alternative is too unpredictable for a manufacturer and the risk of exposure to liability is substantial enough to deter pursuing further development of the product and marketing it, regardless of the benefits to the public.

On the other hand, manufacturers may shield themselves with disclaimers, as mentioned above, under breach of warranty theories of liability. However, this provides too much protection and does not create enough incentive to create a product that reflects the highest safety standards.

By limiting the avenues of liability to negligence, the manufacturers will not be able to waive liability and thus will have the incentive to use the highest safety standards, but they will be shielded from strict liability, so they will better be able to predict liability claims. Burden to the industry will likely be considered as well as the cost and availability of solutions and insurance.[125] This burden will likely be high, since the technology is still in development, and when the car is first marketed, the cost will likely be high and the market may be small. Under a scheme that allows only negligence, a manufacturer will owe a duty of care to a plaintiff, which, as discussed above, may be high considering the nature of this particular product and the reliance that a blind driver would foreseeably place on a vehicle marketed as essentially an assistive device. But the manufacturer may also have an advantage due to the nature of the product, since the dangers of using such a product will be plain and a plaintiff may be deemed to have assumed the risk of using it.

In addition, proximate cause may be difficult for a plaintiff to show. Although the reasoning employed in *Saloomey* works in favor of plaintiffs,[126] Professor Scott's argument that *Saloomey* is different from software security cases because it involves an easily identifiable negligent act points to a difficulty plaintiffs must overcome.[127] While *Saloomey* involved one dedicated function, the car will involve many different interacting technologies facilitated by an operating platform, and it will be difficult to pinpoint the site of a malfunction in order to prove proximate causation. The use of interface technologies and interaction between the vehicle and the driver further complicate the determination of proximate cause where negligence is found on

[125] Barry, *supra* note 10.

[126] *Saloomey*, 707 F.2d at 677.

[127] Scott, *supra* note 80, at 449.

the part of the plaintiff and the defendant. Whereas in *Saloomey* the court was able to assign proximate cause to the manufacturer despite the negligence of several parties, the nature of the interface technology of RoMeLa's ByWire XGV and similar vehicles will make the determination more complex.

C. Regulation of Similar Vehicles and Technology Components

A further barrier, as mentioned above, is that without regulations specifically defining the "rules of the road" for the quasi-autonomous vehicle, manufacturers may be deterred from producing the car. If the car cannot be lawfully utilized on public highways, it will not likely make it to the market. Despite the lack of autonomous and quasi-autonomous vehicles on public highways, standards exist for specific types of autonomous vehicles not meant to travel on public roads. Unfortunately, they are limited in scope and may provide little meaningful guidance. For example, the American Society of Mechanical Engineers' ("AMSE") / American National Standards Institute ("ANSI") Standards regulate automated functions in trucks.[128] American National Standard B56.5 applies to unmanned, automatic guided industrial vehicles, automated functions of manned industrial vehicles, and industrial vehicles modified to operate in an unmanned, automatic mode.[129] The 2005 Standards include design, construction, and testing condition standards for the manufacturer[130] and operation standards for the user.[131] Because the standards apply only to industrial use, the main problem with applying them to regulations for

[128] Industrial Truck Standards Development Foundation, ASME B56.5, Safety Standard for Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles [hereinafter ASME B56.5 Safety Standards].

[129] *Id.* at 1.

[130] *Id.* at 7.

[131] *Id.* at 5-6.

quasi- or fully autonomous cars, is that as Professor Brenner points out, regulations designed for the professional do not translate to regulations for pervasive technology—that is, technologies designed for use by the lay user, as non-industrial cars are contemplated to be. However, these regulations give some frame of reference for the basic categories of concern—such as general safety practices in automated vehicles or automated functions like handling of emergency stopping features, changes in environment, changing of batteries, warning and safety devices, installations, override features, and diagnosis and repair.[132]

In addition, the Department of Commerce's National Institute of Standards and Technology ("NIST") developed the Industrial Autonomous Vehicle Project ("IAVP") to "further the intelligence of vehicle platforms for navigation via measurements, standards and advanced technology developments.""[133] The IAVP includes both military and DOT projects.[134] The projects deal with the development and advancement of standards and measurements in autonomous vehicles.[135] For example, NIST worked as one project goal to clarify ASME's Standard ASME B56.5a-1994 regarding the definition of non-contact bumpers, i.e. laser sensors.[136] Another project involved developing vision-based technology to allow autonomous vehicles to follow lanes.[137] Although many of the standards are directed toward industrialized vehicles, as are the ASME standards, the standards may be helpful in the design and

[132] ASME B56.5 Safety Standards, *supra* note 128, at 3-5.

[133] Roger Bostelman, Maris Juberts, Sandor Szabo, Robert Bunch and John Evans, National Institute of Standards and Technology, Department of Commerce, *Industrial Autonomous Vehicle Project Report*, NISTIR 6751, June 7, 2001, *available at* http://www.isd.mel.nist.gov/projects/iav/index.htm.

[134] NIST, *Industrial Autonomous Vehicle Project*, Oct. 2, 2006, *available at* http://www.isd.mel.nist.gov/projects/iav/index.htm.

[135] Industrial Autonomous Vehicle Project, *supra* note 134, at 2.

[136] *Id.* at 3.

[137] *Id.* at 5.

manufacturing of the specialized cars as safety and regulation of the field become a crucial factor.

Also pertinent to that consideration are the SAE Aerospace Standards, developed by the AS-4 committee.[138] The AS-4 committee is a joint endeavor of the Joint Architecture for Unmanned Systems Working Group ("JAUS WG"), commissioned by the Office of the Undersecretary of Defense, Acquisition, Technology, and Logistics, Strategic & Tactical Systems/Land Warfare and the SAE.[139] The main objective of the SAE AS-4 committee is "to publish standards that enable interoperability of unmanned systems for military, civil and commercial use through the use of open systems standards and architecture development."[140] Four subcommittees address the specific areas of Architecture Framework, Network Environment, Information Modeling and Definition, and Performance Measures.[141] Once again, although these standards may prove very useful for the industry and may provide some frame of reference for developing regulatory standards, these measures are specifically formulated for a specialized and contextual use, and will be of little use to non-specialist users.

More relevant is state recognition of autonomous vehicles. Last year, Nevada became the first state to "legalize driverless vehicles, and laws to the same effect have been introduced in Florida and Hawaii."[142] The Nevada law in question defines an "autonomous vehicle" as "a motor vehicle that uses artificial intelligence, sensors and global positioning system coordinates

[138] SAE International, SAE AS-4 Technical Committees – Unmanned Systems, 2011.

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] Markoff, *supra* note 1.

to drive itself without the active intervention of a human operator."[143] Section 482A.100 of the law authorizes and mandates the Department of Motor Vehicles to adopt regulations for the operation of autonomous vehicles on state highways.[144] The regulations must (1) establish requirements autonomous vehicles must meet before they may travel on state highways; (2) establish requirements for the insurance that is required to test or operate autonomous vehicles on state highways; (3) set minimum safety standards for autonomous vehicle and their use; (4) provide for testing of such vehicles; (5) restrict testing to certain geographic locations; and (6) establish any other requirements the Department deems necessary.[145] The Nevada state model may be helpful in beginning to develop a scheme for general state-by-state regulation of quasi-autonomous vehicles, but the question of how cars developed for blind drivers should be regulated leaves open many questions. Should insurance requirements be the same or heightened for blind drivers and cars marketed for this purpose? Are minimum safety standards the same for autonomous cars and for cars developed for blind drivers? Once again, does the degree of "active intervention of a human operator", as the statute defines it, make all the difference?

D. Formulating Regulations for Licensure, Ownership, and Operation

The regulations must be formulated, as the Nevada statute suggests, to cover vital areas of safety that autonomous vehicles and features implicate but manual driving does not. A vehicle based on interface technologies for blind drivers requires more. These regulations must be carefully designed to address safety issues that may arise from the ownership and operation of

[143] NEV. REV. STAT. § 482A.030 (2011).

[144] NEV. REV. STAT. § 482A.100(1) (2011).

[145] NEV. REV. STAT. § 482A.100(2) (2011).

the vehicle on state highways as well as local roadways.[146] For example, the regulations may set forth driver test requirements in order to ensure that drivers are adept at operating the interface technologies and features with which the car is equipped. The test should be tailored to test the driver's ability to interact with and operate the features of the car in conditions generally required by state licensing agencies, along with other driving challenges the agencies may choose to impose, such as to drive through conditions designed to test the features with which the car is enhanced. However, caution must be taken that any driver examination tests the ability to use the features safely, and does not unfairly disadvantage blind or visually impaired drivers.

The test should be an evaluation of ability to use the car to drive safely commensurate with the standards now used to test drivers' abilities with manually operated cars. Such a test should be used to contemplate some flexibility for evolving technology, but base the evaluation in basic safety standards. State variations will exist, but similarities will revolve around these basics. There is also a question of reasonable modification for drivers with visual impairments. In the case of the car itself designed for blind drivers, however, it could be argued, as discussed above, that the car is itself an assistive device. But since the function of licensure is not limited to use of the technology, but includes driver education and issuance of a driver test, it involves a state service. So under the ADA a reasonable modification is a consideration, provided and assuming it does not fundamentally alter the state service.[147] If these services are offered on a standard formulated to be equally accessible to individuals with and without disabilities, the question is most easily resolved. Although the states may legitimately impose vision

[146] At present, the Nevada statute only addresses state highways. *See* NRS 482A.030 (2011).

[147] 28 C.F.R. § 35.130 (2011).

requirements, they must be grounded in a safety requirement.[148] Therefore, if it can be determined that operation of the RoMeLa car, for example, is safe without a vision requirement, a public entity would be prohibited from barring blind individuals from obtaining licenses to drive those vehicles if there were regulations governing the licensure and operation of these cars.[149]

One possibility for implementing a regulatory scheme is to begin with a pilot program. State legislatures may choose to adopt statutes such as the Nevada statute, tailored toward quasi-autonomous vehicles with interface technologies for blind drivers and devise pilot regulation programs for bringing the vehicles to the roads. For example, the program may start by restricting such cars to single, dedicated lanes, as carpool lanes are presently used, on major highways, and slowly integrating into larger traffic patterns. In addition, there may be some restricted driving areas that prohibit use of autonomous and/or quasi-autonomous vehicles, which may address some of the concerns analysts have identified with each, both on practical and legal/regulatory terms. By beginning with a pilot "test" program and slowly expanding, lawmakers will have an opportunity to test out what many experts in the field now predict to be a reality—that autonomous, and even driverless cars will populate the roads in the near future. Allowing quasi-autonomous interface technology cars to play a role in that evolution of

---

[148] *See* AA Title II Technical Assistance Manual II-3.7200, *available at* http://www.ada.gov/taman2.html#II-3.4400 ("An individual is not "qualified" for a driver's license unless he or she can operate a motor vehicle safely. A public entity may establish requirements, such as vision requirements, that would exclude some individuals with disabilities, if those requirements are essential for the safe operation of a motor vehicle.").

[149] *See id.* ("The public entity may only adopt "essential" requirements for safe operation of a motor vehicle. Denying a license to all individuals who have missing limbs, for example, would be discriminatory if an individual who could operate a vehicle safely without use of the missing limb were denied a license. A public entity, however, could impose appropriate restrictions as a condition to obtaining a license, such as requiring an individual who is unable to use foot controls to use hand controls when operating a vehicle.").

technology will ease the transition and promote further participation of individuals with visual disabilities in the everyday activity of driving, a substantial move forward in independent travel.

V. Conclusion

With the introduction of legislation to regulate autonomous vehicles on public highways and the increased testing of these cars, it is credible that a vehicle designed to facilitate independent driving for blind individuals might be marketable. The technology that the only car currently being developed for such a purpose—RoMeLa's customized XGV—could bring to the public would benefit blind and sighted individuals, increase driving safety, and enhance products currently on the market. The danger that liability poses to manufacturers could be a major deterrent, however, presenting a disincentive to designing and producing the vehicles. Strict products liability theories are particularly dangerous because of the low burden the plaintiff must meet in order to prevail. In direct contrast, breach of warranty claims may be too lenient because if manufacturers can waive their liability through disclaimers they may not be given enough incentive to exercise care and to hold themselves to the highest standards of safety. By limiting applicable liability theories to negligence, manufacturers will have an incentive to strive for the highest safety standards but will also have some predictability in assessing liability claims, and will not be unfairly burdened by a strict liability system. In addition, by adopting a regulatory system that is crafted to meet the safety requirements and practical considerations of the quasi-autonomous car, perhaps looking to the Nevada statute as a model for the necessary areas that should be addressed by regulations, states may open the door further for manufacturers, since there is little incentive to create a vehicle that cannot be driven legally on the public roads. Once these barriers are cleared, the introduction of the quasi-autonomous vehicle will improve life for

countless individuals nationwide. To do so will further the objectives of federal disability law and enhance safety, efficiency, and innovative automobile technology for all drivers.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 3, PAGE 65

U.S. Export Controls Over Cloud Computing: The Forecast Calls for Change

Ryan M. Murphy*

TABLE OF CONTENTS

INTRODUCTION 66
I. U.S. EXPORT CONTROL LAWS AND REGULATIONS 68
II. OVERVIEW OF CLOUD COMPUTING 71
A. *Cloud Computing Service Models* 72
B. *Cloud Computing Deployment Models* 74
III. U.S. GOVERNMENT'S RESPONSE TO EXPORTATION VIOLATIONS IN THE CLOUDS 75
A. *2009 BIS Advisory Opinion* 76
B. *2011 BIS Advisory Opinion* 77
C. *Cloud Computing Implications Under EAR's Advisory Opinions* 78
D. *Any Guidance from Outside the BIS?* 82
E. *Where to Go from Here?* 82
IV. THE EUROPEAN MODEL FOR EXPORT LAW AND CLOUD COMPUTING 82
A. *United Kingdom's Export Control Act of 2002 and Its Effect on Cloud Computing* 83
B. *European Union's Regulation 428/2009 and the Green Paper on Dual-Use Controls* 87
V. RECOMMENDATIONS FOR THE FUTURE OF U.S. EXPORT CONTROLS ON CLOUD COMPUTING 89
CONCLUSION 91

INTRODUCTION

Are you violating United States export law when you click "save" on that document? Exactly where does that file go? For some, it may travel to a server within their company's building, but for an increasing population, that file goes "into the clouds" and out of the country. If you use a service provider to host e-mail or store data, it's important to understand the type of data you are storing and where that information is located. Many cloud providers utilize a vast array of servers, referred to commonly as "clouds", located all over the world.[1] These servers are connected and work together to provide a seamless hosting environment for users.[2] A significant export control issue arises when the data stored on a cloud falls within the type regulated by the Export Administration Regulations ("EAR"), and it's sent to a server in another country.[3] If so, you may have just unknowingly exported your data and become subject to government regulation.

With the global market for cloud computing services projected to grow from $68 billion in 2010 to almost $150 billion in 2014 and the Obama administration's plans to move a significant portion of its IT capabilities to a cloud within 14 months,[4] there is a great need for reform in the United States' outdated export law. The United States enacted the current Export

---

* Syracuse University College of Law, Juris Doctorate Candidate 2013

[1] Tom Reynolds, *Cloudy Answers on Cloud Computing*, http://www.exportsolutionsinc.com/blog/cloudy-answers-on-cloud-computing/ (last visited Feb 6., 2012).

[2] One day your data may be located in Massachusetts, the next day it may be sent to a server in Amsterdam, and the next day sent to a server in India and so on.

[3] This applies even if an e-mail is sent from a United States location through a foreign server to another United States location.

[4] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

Administration Act ("EAA of 1979") in 1979, and has made no significant change since. In fact, EAA of 1979 has been expired for a significant time, but regulations created under it remain in force pursuant to a separate emergency power statute.[5] Since 1979, our society has become fully integrated with technology and the vast majority of businesses now use computers, e-mail, and the Internet daily. We are no longer the society cut off from the world we once were in 1979, but our current law does not reflect this evolution.[6] From this, a tension exists between cloud computing and export control that must be handled in a way that allows cloud computing to reach its potential, but still gives reasonable protections to the United States.

Part I of this Note frames the issue by providing relevant background information on the development and current landscape of U.S. export control laws. Part II then provides a detailed overview of cloud computing and the different options a business has in its use of the technology. Part III examines the current application of U.S. export control law on cloud computing and discusses implications that may arise in different scenarios. In Part IV, this Note looks to the United Kingdom and the European Union and gleans potential initiatives the U.S. government should implement to revise the outdated U.S. export control law. Part V posits three specific fixes the government must implement to correct the U.S. export control system. Lastly,

---

[5] 50 U.S.C. § 2419 (2013); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 324 (2004); International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1707 (2013).

[6] See Advisory Opinion from C. Randall Pratt, Director, Information Technology Controls Center, Office of National Security and Technology Transfers Control, Bureau of Industry and Security (Jan. 11, 2011) (available at http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan11_2011.pdf) and Advisory Opinion from C. Randall Pratt, Director, Information Technology Controls Center, Office of National Security and Technology Transfers Control, Bureau of Industry and Security (Jan. 13, 2009) (available at http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan13_2009_ao_on_cloud_grid_computing.pdf) (two advisory opinions have been given on the effect cloud computing has had on the meaning of the term "export," but no unified position has been given by the government).

this Note concludes by recommending the complete revamping of U.S. export control law in order to create a more efficient system that will allow cloud computing to reach its full potential.

I. U.S. EXPORT CONTROL LAWS AND REGULATIONS

The U.S. Constitution vests Congress with the power to "regulate commerce with foreign nations."[7] Specifically, this clause of the Constitution gives Congress power to regulate the exportation of domestic goods abroad. With this ability, Congress passed the EAA of 1979 and the International Emergency Economic Powers Act ("IEEPA").[8] These acts authorized multiple federal agencies, namely the Department of Commerce, to oversee and to regulate the exportation of commodities, software, and technology.[9] It is important to note, however, that the act terminated on September 30, 1990, but President Bush issued an executive order to extend it in its original form until Congress produced new legislation (which has still yet to occur).[10] Congress had three major goals when they passed EAA of 1979: enhance national security,[11] allow for the use of exports as a foreign policy tool, and restrict exports in short supply.[12]

---

[7] U.S. CONST. art. II, § 8.

[8] EAA of 1979, 50 U.S.C. § app. 2403; the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1707.

[9] *Id;* Karen R. Smith, *A Basic Discussion of U.S. Export Regulations: What Every Client Needs to Know*, 1 J. TRANSNAT'L L. & POL'Y 113 (1992) ("The federal government regulates all exports, and authority for overseeing and regulating exports is divided among a number of agencies . . . the Department of Commerce, [] is a 'catch all' agency charged with regulating virtually all exports not regulated by any other agency . . . .").

[10] *See* 15 C.F.R. § 770.3(a) (1991)*;* Exec. Order No. 12,730, 3 C.F.R. §305 (1991).

[11] Karen R. Smith, *A Basic Discussion of U.S. Export Regulations: What Every Client Needs to Know*, 1 J. TRANSNAT'L L. & POL'Y 113 (1992) (National Security encompasses products that contribute to the military potential of any other country which hurt U.S. national security, such as software, computers, and electrical equipment. This is closely tied to foreign policy restrictions.).

[12] 50 U.S.C. app. § 2402(2); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 329 (2004).

Though multiple agencies regulate the exportation of domestic products since the passing of the EAA of 1979, the Department of Commerce has lead the government's enforcement and regulation of non-physical exports today. Specifically, the Department of Commerce's Bureau of Industry and Security ("BIS") administers the specific regulations implemented by the EAA of 1979.[13] These regulations are administered through the use of EAR.[14] The US government, however, does not actively enforce the regulations defined in the EAR.[15] The EAR only recommends parties involved in export transactions analyze the nature of the product they are exporting and then determine, on their own, whether a license[16] would in fact be required.[17]

The EAR defines an export as "an actual shipment or transmission of items [including technology or software subject to the EAR] out of the United States."[18] Additionally, the EAR provides that "an actual shipment *or transmission* of items subject to the EAR out of the United States, or *release of technology or software* subject to the EAR to a foreign national in the United States . . ." (emphasis added).[19] Further, BIS maintains a list of the technologies subject to the

---

[13] Bureau of Industry and Security Export Administration Regulations, 15 C.F.R. §§ 730-774.

[14] *Id.*

[15] *See* 15 C.F.R. §§ 732.1(b)-(c); Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 332-33 (2004).

[16] 15 C.F.R. § 770.3(a) (1991) ("[T]he export from the United States of all commodities, and all technical data . . . is hereby prohibited unless and until a general license authorizing such export shall have been established or a validated license or other authorization for such expert shall have been granted . . . .").

[17] Gregory W. Bowman, *E-Mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 332-33 (2004).

[18] 15 C.F.R. § 772.1 (2013) (The term "subject to the EAR" is a defined term of art in the EAR used "to describe those commodities, software, technology, and activities over which [BIS] exercises regulatory jurisdiction under the EAR.")

[19] 15 C.F.R. §734.2(b)(1) (2013).

EAR.[20] This list is known as the Commerce Control List ("CCL"), and is contained within the EAR.[21] The restrictions on items listed in the CCL depend on the location where the item is being exported or the nationality of the person to whom it is being sent.[22]

To clarify its regulations, the EAR puts forth five questions for exporters to consider when determining the need for a license: (1) is the item subject to the EAR; (2) how is the item classified for EAR purposes; (3) what is the item's ultimate destination; (4) what parties are involved in the transaction and are any of the parties restricted; and (5) what is the intended end use of the item?[23] The EAR applies to all civilian and "dual use"[24] commodities,[25] software,[26] and technology[27] not publically available.[28] In essence, the government shifts the burden to comply with the regulations set forth in EAR onto the exporter. Though self-regulating, the penalty for violating the EAR can range up to $50,000 and/or imprisonment for up to five years.[29]

---

[20] 15 C.F.R. §738.1 (2013).

[21] 15 C.F.R. §774 (2013).

[22] 15 C.F.R. §738.1 (2013).

[23] Gregory W. Bowman, *supra* note 17 at 333-34.

[24] *See* 15 C.F.R. § 772.1 (2013) (dual use refers to "[i]tems that have both commercial and military or proliferation applications.").

[25] *Id.* (EAR defines commodity as "[a]ny article, material, or supply except technology and software").

[26] *Id.* (EAR defines software as a "collection of one or more 'programs' or 'microprograms' fixed in any tangible means of expression.").

[27] *Id.* (EAR defines technology as "[s]pecific information necessary for the 'development', 'production', or 'use' of a product," and this information can "take[] the form of 'technical data' or 'technical assistance.'")

[28] Bowman, *supra* note 17 at 319, 334.

[29] *See* 15 C.F.R. § 764.3(b).

II. OVERVIEW OF CLOUD COMPUTING

Cloud computing[30] describes the use of technology that allows users to access services over the Internet without the need to control the infrastructure that provides the services.[31] In essence, it is computing on demand that makes applications and storage from remote computers accessible at anytime and from anywhere.[32] In public or community clouds (the focus of this note), a third-party vendor ("provider") owns or controls the remote hardware, software, and facilities[33], and the cloud computer user ("user") may access or upload that data anywhere and at any time. To be specific, providers offer services, such as server space or tools for software development, to the public and users can be individuals, companies of any size, or government agencies.[34] Common examples of public cloud services are e-mail message storage on remote servers by companies such as Google, Web 2.0, and services such as Facebook that provide storage of social networking information.[35]

---

[30] The term cloud computing "comes from the early days of the Internet where we drew the network as a cloud . . . we didn't care where the messages went . . . the cloud hid it from us." Kevin Marks, Google

[31] 14 No. 5 CYBERSPACE LAW 1; *See, e.g.*, *In re* Google, Inc. & Cloud Computing Servs. (Mar. 17, 2009) ("Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices."), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf; Robert Gellman, World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, 4 (2009) ("[C]loud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections.").

[32] 14 No. 5 CYBERSPACE LAW 1.

[33] Shannon Brown, *Navigating the Fog of Cloud Computing Cloud Computing May Raise Ethical Questions. It Also Requires Technical Competence. Are You Ready?*, PA. LAW., September/October 2011, at 18, 19.

[34] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012).

[35] *Id.*

Cloud computing has become a popular alternative for business because of a cloud's scalability, virtualized resources, and portability.[36] This is because the cloud's routers, servers, and technical data storage devices are generally located across multiple systems and taken care of by a third-party.[37] In fact, most companies generally do not know where their data will be stored within the cloud.[38] Cloud computing services are analyzed in the context of two important models of categorization: service models and deployment models.[39]

A. *Cloud Computing Service Models*

Clouds may be classified into different categories by the functions they perform for the user. Four standard types of "Service Models" currently exist[40]: Software-as-a-Service ("SaaS"), Storage-as-a-Service ("STaaS"), Platform-as-a-Service ("PaaS"), and Infrastructure-as-a-Service ("IaaS")[41]. SaaS and StaaS will be the focus of discussion in this note because of the public nature of the provider. While Paas and Iaas are important in the field of cloud computing, they do not deal with public use[42] and will therefore not be discussed in detail.[43]

---

[36] *The Export Control Implications of Cloud Computing*, *supra* note 4.41 No. 17 THE LAWYER'S BRIEF 2.

[37] *Id.*

[38] *Id.*

[39] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, SPECIAL PUBLICATION 800-145, *The NIST Definition of Cloud Computing* (September 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[40] Providers have the option to combine any attribute from the four types available to create a hybrid.

[41] Shannon Brown, *Navigating the Fog of Cloud Computing Cloud Computing May Raise Ethical Questions. It Also Requires Technical Competence. Are You Ready?*, PA. LAW., September/October 2011, at 18, 19 (2011).

[42] 14 No. 5 CYBERSPACE LAW 1 (IaaS allows people to rent services such as processing, storage and network capacity and PaaS allow developers to create applications that run in and use services provided from the cloud).

SaaS and STaaS provide users with two different, but important abilities. First, SaaS allows for organizations to pay for the use of servers to store their software application for third-party desktop users to access (for a price) without having to install the software.[44] In this model, the user does not control the underlying cloud infrastructure (i.e. the network, servers, operating systems, storage).[45] An example of this service model may be seen in Google Apps. In Google Apps, companies may upload their software onto Google's server for a cost and then Google allows for the public to access the software without forcing them to download it onto a computer.[46]

On the other hand, STaaS allows for online backups, data synchronization and file storage with sharing capabilities.[47] This type of cloud allows for users to backup data on a third-party server and creates the ability to access that information from mobile electronic devices.[48] An example of this service model may be seen in Apple Computer's MobileMe. MobileMe allows for individuals to backup their data stored on a personal computer and then access that data from anywhere at any time.[49]

---

[43] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011) (PaaS: "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider") (IaaS: "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software").

[44] 14 No. 5 CYBERSPACE LAW 1; Brown, *supra* note 41, at 18-19.

[45] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[46] *See* http://www.google.com/apps/intl/en/business/index.html (last visited Feb. 7, 2012).

[47] Brown, *supra* note 41 at 18, 19.

[48] *Id.*

[49] *See* http://www.apple.com/mobileme (last visited Feb. 7, 2012).

B. *Cloud Computing Deployment Models*

A cloud may also be categorized through the way in which it is shared (or not) between different users. There are four different "deployment models" a cloud may be defined as: a private cloud, a public cloud, a community cloud, and a hybrid cloud.[50]

In a private cloud, the infrastructure is owned by, or operated for, a single user. This cloud may, however, be owned, managed, and operated by the organization, a third party, or a combination of the two.[51] The location of the cloud may exist on or off the premises.[52]

In a public cloud, however, the infrastructure is open to the general public and shared between multiple unique users.[53] This open cloud means the users will be forced to operate the same hardware and software within the same database.[54] This model exists on the premises of the cloud provider.[55] A common example of such a cloud may be seen with e-mail servers such as Google or with data storage such as Apple's MobileMe.

In a community cloud, the third type of deployment, the infrastructure is owned by and operated for a limited set of users.[56] These users, such as a national government, generally hold

---

[50] W. Kuan Hon & Christopher Millard, *Data Export in Cloud Computing, How can Personal Data be Transferred outside the EEA?*, Queen Mary University of London School of Law Legal Studies Research Paper No 85/2011, available at: http://ssrn.com/abstract=1925066 (last visited Feb. 6, 2012).

[51] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011).

[52] *Id*.

[53] Kuan Hon, *supra* note 50. See also, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[54] *Id*.

[55] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[56] Kuan Hon, *supra* note 50.

a common interest (e.g., mission, security requirements, and compliance considerations).[57] For example all Government organizations within the state of Massachusetts may share computing infrastructure on the cloud to manage data related to citizens residing in Massachusetts.

In a hybrid cloud, the infrastructure is owned and operated for a specific user, but when necessary the user may process activities in a public cloud.[58] This cloud may be owned, managed, and operated by the organization, a third party, or a combination of the two.[59] The location of the cloud may exist on or off the premises.[60]

III. U.S. GOVERNMENT'S RESPONSE TO EXPORTATION VIOLATIONS IN THE CLOUDS

With the boom in technology from the enactment of the EAA of 1979, regulation of exports has attempted to expand with it. This has shown itself in the widening types of goods deemed to be exports as well as tweaks to the language within statutes to encompass non-tangible goods such as software.[61] Though multiple government agencies regulate domestic exports in the United States, only the BIS has attempted to answer the mounting questions swirling around cloud computing technology.[62] Specifically, the BIS issued two advisory

---

[57] Kuan Hon, *supra* note 50.

[58] *Id.*

[59] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[60] *Id.*

[61] *See* 15 C.F.R. § 770.

[62] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

opinions on cloud computing in 2009 and most recently in 2011.[63] With confusion created from the seemingly unknown new technology, these opinions were intended to guide the public in the application of EAR guidelines regarding technology products in the clouds.[64] However, it is important to note that these advisory opinions are not binding law, and only the BIS's perspective on the potential legal issues that may arise with cloud technology.

A. *2009 BIS Advisory Opinion*

BIS first submitted an advisory opinion ("2009 AO") on the application of the EAR to cloud computing technology in 2009.[65] In this opinion, BIS commented on some basic definitional issues and made it quite clear the user, and not the provider, of the cloud technology will be responsible for abiding by EAR.[66] In essence, 2009 AO made four important comments on cloud technology.[67] First, BIS stated that providing cloud technology is not an export nor is it subject to EAR.[68] Second, a user transmitting controlled software to a foreign destination[69] to enable cloud computing is subject to the EAR.[70] Third, exporting controlled software or

---

[63] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[64] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[65] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[66] *Id.*

[67] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[68] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[69] This also applies to transmitting software to a foreign national within the US and the routing of software through a foreign location.

[70] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

technology to and from a cloud is subject to the EAR.[71] Fourth, the cloud provider in the US is not the exporter of any data that users place on and retrieves from their cloud.[72] Analyzing this advisory comment in light of the EAA of 1979 and the EAR, BIS makes its desire for self-regulated compliance quite clear. BIS's 2009 AO again puts the onus on the user to stay within the export laws and seemingly leaves them out in the rain.

B. *2011 BIS Advisory Opinion*

In January 2011, BIS submitted a second advisory opinion, but this comment focused on whether cloud providers need to obtain "deemed export" licenses[73] for their foreign national IT administrators who have access to the users' controlled technology ("2011 AO").[74] Generally under EAR, a foreign national, even when within the boarders of the United States, must have a license approved by the BIS in order to access certain products deemed restricted. However, in the 2011 AO, BIS determined this regulation did not pertain to the provider of the cloud.[75] With seemingly no regulations on the provider, the 2011 AO stretches the responsibilities of the user even more. In essence, because the provider has no culpability in regards to the product being

---

[71] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[72] *Id.*

[73] *See* 15 C.F.R. §734.2(b); Bowman, *supra* note 17 at 319, 338-40 ("[I]n addition to applying to physical and non-physical exports and re-exports, the EAR also expressly state that a 'release' of 'source code' software or technology to a foreign national who is not a permanent resident of the United States or a protected individual under U.S. immigration laws is deemed to be an export to the foreign national's home country [last country of citizenship or permanent residence], even when the release occurs entirely within national borders.").

[74] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011); Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[75] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

stored on their server or routed through their system, it becomes the responsibility of the user to ensure that its data is not accessible by any foreigners.[76]

C. *Cloud Computing Implications Under EAR's Advisory Opinions*

Both advisements have provided insight into the BIS's perspective on legal issues created by cloud computing technology, but they only addressed a limited range of scenarios. The main lesson to glean from these advisements is this: the sole burden of compliance with the EAR falls onto the *user* of cloud computing services and *not* the provider.[77] Each of the Advisory Opinions has its own subtle comment on this major fact and each address it at a different angle.

In the 2009 AO, the BIS provides that the provider is *not* an exporter because providing computational capacity, by itself a service, does not qualify as an exportation because it does not receive "the primary benefit of the transaction."[78] For example, if a U.S. based company decides to use a cloud provider that happens to have their servers based in the Netherlands, they will be responsible for this "export" even though they did not intend to export any product but only put the product on the third-party server to store it. However, according to the BIS, the company in this situation receives the primary benefit of this export and therefore has the obligation to abide by the U.S. export control laws and is responsible from protecting the data or product from foreign entities. In fact, the provider does not even have an obligation to inform the user of the location of their servers and if they reside outside of the United States.[79]

---

[76] This includes even the provider's own employees; Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[77] *See* BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[78] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[79] *Id.*

The BIS addressed a similar issue in their 2011 AO. In it, the BIS broke down the obligations of users and providers when dealing with the provider's own foreign employees and tackled the question of who had the onus to protect technology from "deemed exports."[80] The issue arose from cloud providers and their foreign IT administrators' potential use of the user's data or product (which would be a deemed an export within or outside of the United States).[81] In this scenario, the 2011 AO, again, essentially put the entire burden on the user to protect their data or product from the provider's potentially foreign employees.[82]

These base rules taken from the Advisory Opinions create issues for the user in four different situations: (1) the provider's servers or resources are abroad and the user is in the United States; (2) the provider's servers or resource are in the United States and the user is abroad; (3) provider's servers or resources and the user are out of the United States; and (4) provider's servers or resources and the user are in the United States.[83]

The first, most common, scenario where the provider is based abroad but the user is within the United States will require the standard application done with similar electronic exports of technology or software. Essentially, if the user transmits controlled data to a cloud a standard export has occurred and the user must make sure that they comply with the EAR and undertake the proper process to receive a license for the product. With this scenario, the provider has no obligations to inform the user of potentially foreign locations of servers.

---

[80] BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[81] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[82] *Id.*; *see also* BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

[83] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012); *see* BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009); BIS ADVISORY OPINION ON CLOUD COMPUTING, 992 PLI/Pat 982 (2011).

Second, another scenario may occur where the user is based abroad and the provider's servers are within the United States. Here, the guidelines by BIS become murky and we are forced to imply certain aspects of their opinions. Essentially, the 2009 AO clarified that providing a cloud service is not an activity subject to the EAR, but if that provider transmits controlled data to the user abroad, an export has occurred nonetheless. The provider, the BIS reasons, would not be responsible because they would not receive the "primary benefit . . . of the transaction," but who then will be responsible?[84] We may attempt to assume the BIS's meaning, but that would most likely be unfruitful with such a brief analysis on their part. In the end, this scenario shows BIS acknowledging that the EAR does not yet address how to deal with this situation.

Extending from the second scenario, a similar situation may arise if both the provider and the users are outside of the United States but dealing with U.S.-origin software or technology. For example, this issue may occur if a user, based in Turkey, decided to store data created within the United States in a cloud based in Scotland. In other words, this deals with the issue of re-exports.[85] The issue from the previous scenario comes back into play here. The BIS fails to address who would be responsible for this when dealing within the framework of cloud computing. Some analysts of the Advisory Opinions point to this also hinting at the lack of responsibility the provider in this situation would hold.[86]

Under the fourth scenario, the provider and the user are both within the United States, but the data or product is considered a "deemed export" because a foreign national has obtained it

---

[84] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[85] *US Export Controls and Cloud Computing*, LAW360, published September 10, 2010, available at http://www.law360.com (last visited Feb. 6, 2012) (U.S. origin product or data exported from one foreign country to another).

[86] *Id.*

from the provider. For example, if a U.S. based company uploads their product onto a cloud, such as Google Apps, and from there the product is downloaded and used by a foreign national. A situation may also arise in this scenario, with the same result, where an IT professional for the provider uses the product and it will still be considered a deemed export. The BIS has clearly stated the onus will be on the user in this situation, and it will be its responsibility to comply with the U.S. export control laws.[87]

With all the varying regulations forced upon the user, and the user alone, to comply with the export laws, cloud computing creates a huge potential for individuals and companies alike to inadvertently violate export control laws. Companies and individuals may be able to protect themselves from these nuances in export control law, but the burden is great and uneven. In a comprehensive article by Alexandra Lpez-Casero, she sets forth seven methods for users to protect themselves with the BIS comments in mind: (1) have a good command of the regulatory regimes, export control classifications, and licensing requirements applicable to their data or product; (2) Understand and seek out what will happen to the data or product once it is in the cloud; (3) incorporate cloud computing into company-wide policy; (4) review the agreement with the provider; (5) agree with the provider for clouds in limited geographic regions; (6) limit cloud use to items not subject to EAR; and (7) make sure the provider has policies in use to prevent foreign IT administrators from using the data.[88]

[87] BIS ADVISORY OPINION ON CLOUD COMPUTING, 984 PLI/Pat 985 (2009).

[88] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

D. *Any Guidance from Outside the BIS?*

Simply put, no. No other agency has made any comment on the way in which to best regulate the emerging cloud technology. For example, even though the State Department's Directorate of Defense Trade Controls ("DDTC") and the Treasury Department's Office of Foreign Assets Controls ("OFAC") have regulatory functions over domestic exports[89], neither has provided any guidance.[90]

E. *Where to Go from Here?*

Though informative, these Advisory Opinions are only that: opinions. The BIS does not speak for any other organization that controls U.S. exports, and therefore the law is still murky and in flux. Though the compliance methods laid out by Alexandra Lpez-Casero will help in the prevention of potential export control violations, it is only a temporary solution. Therefore, it is imperative that the government addresses cloud computing technology in an official manner through legislation. In fact, other governments, namely The United Kingdom and the European Union, took this step and have begun looking at how to handle these tangled and complicated issues. It would be quite informative to analyze their law as well as the style in which they enacted it.

IV. THE EUROPEAN MODEL FOR EXPORT LAW AND CLOUD COMPUTING

Without significant reform since the passing of EAA of 1979, the U.S. legislature needs to update their export control laws to properly reflect the changing climate of exportation. Though the United States has yet to make this significant step, other governments have begun the

---

[89] Nixon Peabody, *The Export Control Implications of Cloud Computing*, 41 No. 17 THE LAWYER'S BRIEF 2.

[90] *Id.*; Bowman, *supra* note 17 at 319, 334.

process with recent enactments attempting to clear the air and focus their laws on the changing marketplace.[91] In order for the United States to take the next step in regulating the exportation of technology through cloud computing, it would be greatly beneficial to see the style in which these foreign entities attempt to reign in the confusion swirling around cloud computer regulations. In this section, we will be reviewing and analyzing the export regulation of intangible items, such as those within cloud computing technology, in both the United Kingdom as well as within the larger European Union.

A. *United Kingdom's Export Control Act of 2002 and Its Effect on Cloud Computing*

After years of using an outdated act similar to the United States[92] that dated back to the export control theory "prevent trade with the enemy" (regarding Hitler and his rise to power), the United Kingdom passed the Export Control Act of 2002 ("EAC").[93] In the EAC, the United Kingdom defined an intangible export as the transfer of "software or technology by fax, telephone or other electronic devise."[94] In this context, the EAC defines a technology transfer as "a transfer by any means (or combination of means), including oral communication and the transfer of goods on which the technology is recorded or from which it can be derived."[95] Before

[91] *See* Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm.

[92] *See* Import, Export, and Customs Powers (Defense) Act, 2 & 3 Geo. 6, c. 69 § (9)(3) (Eng.).

[93] Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm; Bryan R. Reed, *The United Kingdom's New Export Control Act of 2002 and its Possible Impact on United Kingdom Universities and Academic Freedom: A Comparison of Export Control in the United States and the United Kingdom*, 8 UCLA J. INT'L & FOREIGN AFF. 193, 216.

[94] 8 UCLA J. INT'L & FOREIGN AFF. 193, 216; *see* The Dual-Use Items (export Control) Regulations (2000) SI 200/2620, available at http://www.hmso.gov.uk/si/si2000/20002620.htm (last visited Feb. 6, 2012).

[95] Export Control Act, 2002, c. 28 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm (last visited Feb. 6, 2012); Reed, *supra* note 94, at 216.

the EAC, the United Kingdom has not attempted to restrict technology transfers as exports,[96] but the enacting of this act pushed them into the forefront of technological export control. However, even with slight amendments to the act as recent as 2008,[97] the United Kingdom seems to be similarly behind on the cloud computing technology boom that has occurred throughout the world.

As stated by within a research paper by members within the United Kingdom government, there were two main purposes for the implementation of new export control laws: "(1) to strict the negative impact of arms trade and (2) to provide a transparent framework for legitimate exporters."[98] In fact, the government sought to "impose controls on the transfer of technology from the U.K. and by U.K. persons anywhere and by any means."[99] This ability to impose controls on technology within the United Kingdom is larger than one may first think because the government cast a wide net by defining technology within this act as "information . . . capable of use in connection with . . . an activity of any other kind whatsoever."[100] By defining technology so widely the EAC seems to give the government a wide discretion on whether to deem a move in the clouds as an export and the haze still swirls around the United Kingdom

---

[96] Reed, *supra* note 93, at 218.

[97] Underbill from 2008, 2006.

[98] Mark Oakes & Tim Youngs, Int'l Affairs and Defense Section, Research Paper 01/64, *The Export Control Bill of 2001-02*, at 3 (2001) available at http://www.parliament.uk/commons/lib/research/rp2001/rp01-064.pdf (last visited Feb. 6, 2012).

[99] *Id.*; 8 UCLA J. INT'L & FOREIGN AFF. 193 FOOTNOTE ("Among other powers listed are the power to: impose controls on technical assistance overseas, apply measures to 'give effect to EU legislation on controls of dual-use items,' initiate new licensing procedures . . . .").

[100] 8 UCLA J. INT'L & FOREIGN AFF. 193, 229; 631 Parl. Deb., H.L. (5th ser.) (2002) (statement of Baroness Miller of Hendon).

without any guideposts. However, the United Kingdom attempted to make the proper step forward by addressing the issue of intangible goods and the effect outdated tangible export control laws have on them. Unfortunately, they too seemingly have fell short on a concise proper control and this leaves the exportation of intangible items on cloud technology vague to say the least.

Though the EAC created an act similar to the EAA of 1979 (after multiple revisions since the EAA of 1979's enactment), the way in which the EAC arrived at the composition and content of the act are worth noting. The system by which they created this act occurred through the submission of Green Papers[101] and White Papers[102] by the United Kingdom government to create the best law for their people.[103] In this particular case, the government released both types of Papers in order to open a debate for the proper way to regulate the transfer of technology.[104] Specifically, the White Paper proposed wide regulations on the transfer of technology and the Green Paper pushed for new controls due to the danger of absolutely no control on the transfer of technology (a situation, luckily, the United States does not find itself in).[105] From that point, the government had an open dialogue with the public and within the legislature. In effect, the government went through a transparent process to create what they believed to be the best law by

[101] A Green Paper is a statement that is designed to stimulate discussion amongst a wide audience; http://www.historylearningsite.co.uk/how_laws_are_made_in_great_brita.htm (last visited Feb. 6, 2012).

[102] A White Paper is a statement of where the government wishes to go in the sense that it is fairly definite in what it thinks is required. http://www.historylearningsite.co.uk/how_laws_are_made_in_great_brita.htm (last visited Feb. 6, 2012).

[103] Reed, *supra* note 93, at 220.

[104] *Id.*

[105] *Id.*; *see also* Consultative Document on Strategic Export Controls, 1996 Cm. 3349; White Paper on Strategic Export Controls, 1998, Cm. 3989, available at http://www.dti.gov.uk/export.control/policy/whitepaper/index.htm (last visited Feb. 6, 2012).

allowing the experts within different fields to weigh in on the affect the act would have on the United Kingdom and abroad.

Another interesting facet to the EAC that the United States does not have within its export control laws is judicial review. In the United Kingdom system of export control the Secretary of State makes all final decisions on whether goods, intangible or tangible, will be considered for regulation.[106] The decision of the Secretary of State however, is subject to the scrutiny of the court system and must pass a balancing test to show he or she has not reached beyond the allotted power to control reasonably exported goods.[107] This balancing test is comprised of four steps: (1) Whether the Secretary has taken all relevant facts and other circumstances into account and dismissed all irrelevant facts; (2) whether the Secretary has identified all apparent interferences and the reasoning behind them; (3) whether the Secretary has considered the justifications for the degree of interferences; and (4) whether the Secretary balanced these justifications and the degree of control against the need to respect the freedom to carry out the identified activity.[108]

Though flawed in its own right, the EAC is important for us to be aware of it and to understand how it was created. By looking into the EAC and seeing the process of how it was formed, the U.S. legislature would have the potential to learn new and informative ways to approach U.S. export control laws that may not have been considered previously. The two approaches of note from the EAC are: (1) the use of the Green Paper and White Paper system; and (2) the introduction of Judicial Review into the process.

---

[106] Export Control Act, 2002, c. 28 §8 (Eng.), available at http://www.hmso.gov/acts/acts2002/20028--a.htm (last visited Feb. 6, 2012).

[107] *Id.*

[108] *Id.*

B. *European Union's Regulation 428/2009 and the Green Paper on Dual-Use Controls*

With the advent of technology in the world of exports, the countries within the European Union ("EU"), or "member states," had a fractured system without any real consistency. In fact, there is no explicit regulation of general cloud computing on a Europe-wide scale.[109] However, there are regulations similar in nature to the exportation of data through cloud computing that would help understand the climate of the European Union and would allow us to garner some incites in our own export control regulations regarding the movement of controlled technology on cloud computing technology.

The closest regulation the European Union has to regulation on exportation through cloud computing can be seen in its recent dual-use[110] exportation legislation. The current dual-use export control guidelines may be found in European Union Regulation 428/2009, but the rules within this are extremely complex and the regulation resultantly varies across the member states.[111] Due to this, on June 30, 2011, the EU Commission (hereinafter "the Commission")[112] released a Green Paper, similar to the aforementioned one in the United Kingdom, discussing the European Union's export control regulations for dual-use items and imploring the public to enter

[109] Jason P. Sluijs, Pierre Larouche & Wolf Sauter, *Cloud Computing in the EU Sphere*, TILEC Discussion Paper, Http://ssrn.com/abstract=1909877 (last visited Jan. 13, 2012).

[110] *Council Regulation (EC) No 428/2009*, OFFICIAL JOURNAL OF THE EUROPEAN UNION ch.1 art.2 (defined dual-use as "items, including software and technology, which can be used for both civil and military purposes").

[111] *Council Regulation (EC) No 428/2009*, OFFICIAL JOURNAL OF THE EUROPEAN UNION; Jacques Bourgeois, *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper* (2011) (last visited Feb. 6, 2012), available at http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=9901.

[112] The executive body of the European Union that is responsible for proposing and creating legislation as well as running the daily operations of the Union, available at http://ec.europa.eu/index_en.htm.

a debate about the proper way of regulating technology exportation.[113] This release of the Green Paper was done in an effort to create new consistent Europe wide regulations.[114]

The Commission focused on six major areas of potential improvement on the system currently in place[115]: (1) the creation of a "common risk assessment" between the member states; (2) increasing the exchange of information between member states; (3) Extending the scope of the European Union's Export authorization; (4) a catch-all control; (5) an integrated internal market for dual-use items; and (6) coordinated enforcement of export control rules.[116]

The actual intent of the Commission, though important in some respects, does not directly apply to the implementation of better U.S. exportation control on technologies. However, the overarching theme presented speaks directly to the issues presenting themselves within the United States. Specifically, the issues regarding the fractured nature of our system and how our regulations are vague and unhelpful to users can be seen in both the European Union and the United States. In fact, simply replace the term "member states," and enter "federal agencies" and one can see the similarity plainly.

The European Union took the next logical step, which the Unites States has yet to fully make, and admitted the system is a broken one and attempted to start the process of a significant overhaul. Once the United States can do that, they will be able to make strides in making an

---

[113] EU Green Paper: *The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world* Brussels, 30.6.2011 COM (2011) 393 final.

[114] Peter Flanagan et al., *Recent Developments in EU Export Controls: EU Green Paper on Dual-use Exports*, EUROWATCH (Oct. 15, 2011), http://www.cov.com/publications/.

[115] *See id.*; Jacques Bourgeois et al., *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper* (July 28, 2011) http://www.wilmerhale.com/pages/publicationsandNewsDetail.aspx?NewsPubId=91593.

[116] Peter Flanagan et al., *Recent Developments in EU Export Controls: EU Green Paper on Dual-use Exports*, EUROWATCH (Oct. 15, 2011), http://www.cov.com/publications/.

efficient, fair system that regulates the exportation of intangible technology. There are too many agencies regulating exportation and an astounding lack of both communication and harmonious regulations. This has created a great deal of confusion, especially with a new system of exportation such as cloud computing.

In addition, the Commission is not doing this overhaul behind closed doors, but openly with the submission of a Green Paper to the public for its consideration. By opening the process to any willing member of the public, namely experts and businesspeople in the fields affected, the Commission has an opportunity to hear from those that know the most about how the legislation should be written and what it should include to make it better for the European Union as a whole.

V. RECOMMENDATIONS FOR THE FUTURE OF U.S. EXPORT CONTROLS ON CLOUD COMPUTING

In order to fix the U.S. export regulation system we must do more than tinker with it. In fact, the correction of our export control system calls for a complete overhaul. This statement is no truer than when discussing the particular export control regulation of intangible items. Specifically, those being exported through cloud computing. To fix the system we must: (1) consolidate the governmental regulation of U.S. export; (2) create a dual accountability system between user and provider; and (3) open up the export control legislation to the public and incorporate them into the creation of the regulations.

There needs to be a consolidation of U.S. export control laws. Currently, there are multiple agencies that regulate the export of intangible technology, and each has different regulations on certain items. With numerous agencies seemingly regulating the same items, only confusion can be created in the marketplace. This confusion will inevitably lead to a chilling

effect on one of the largest growing areas of the economy.[117] Similar to the Commission's Green Paper, where they suggested the creation of Europe-wide export control regulations, the United States needs to bring all the agency regulations into one universal regulation. This unification and synchronization will better allow for the U.S. market to grow and match the rest of the world economy.

An example may be seen just how bad it is in the United States through the AO 2009 and AO 2011 opinions. The BIS, only one organization of many, released an "opinion" on the effects of the EAR export control regulations on intangible items within cloud computing. This non-binding opinion answered few questions and left many doors open. Namely, the issue of every other agency that regulates exportations and how they would deal with cloud computing (frankly, including the BIS itself because of the opinions' non-binding nature). Without clarification on the state of export law on intangible items in clouds, the market will move elsewhere.

As the current system works, the user has the sole burden of making sure every facet of the provider's operations are in compliance with the regulations of U.S. export control law. From the location of the provider's servers to the nationality of its employees and even the safeguards it has if it does in fact have foreign national employees that may cause a deemed export risk. In this scenario, it seems the U.S. government has let the provider go scot-free. This is an unacceptable practice. In order for the system to work properly there must be explicit accountability from all sides of the operation, be it user or provider. With dual accountability, each side of the operation will be upfront with their operations and, in turn, this will cause less confusion and fewer violations.

---

[117] *See* Tim Weber, *Cloud Computing Goes Mainstream*, BBC NEWS (May 5, 2010) http://www.bbc.co.uk/news/10097450.

Following the lead from the United Kingdom and the European Union, the United States should open the process up to the public, namely those experts in the fields that know the best about the needs of the technology marketplace. By doing this, the U.S. legislature will be able to facilitate a conversation to foster the best form of regulation regarding cloud computing would make it transparent and allow for the proper regulations to be created in order for the market to grow without restrain or confusion. Though the legislature may be able to create a standard of regulation that would be workable to a layperson, the ability to take a sample from the experts in the field would ensure a viable law with real world applications. In essence, it will remove the chilling effect that the uncertainty from the current law creates within a technology field that is just beginning to understand cloud computing and what it may do for business.[118]

With these three areas addressed, the U.S. export control regulations would be a much more efficient and transparent system. Further, the use of cloud computing would have the opportunity it needs to grow into the market it is projected to be.

CONCLUSION

This Note argues that the United States export control regulations are outdated and in need of reform, particularly in regards to technology. Applying the United Kingdom's approach, the European Union's intent and the analysis of the 2009 and 2011 AOs, this Note believes a better and more efficient system is possible.

This Note acknowledges that the United States has begun considering reform of its export control system. This reform effort may potentially address the creation of a single export licensing authority, single enforcement agency, single control list, and single information

[118] *See* Cloud Computing Goes Mainstream by Tim Weber, http://www.bbc.co.uk/news/10097450 (Last visited Feb. 7, 2012).

technology system.[119] As part of this effort, the United States recently has introduced new export license exceptions, new control categories, and given guidance on issues such as the handling of disclosures of controlled technologies to dual nationals.[120] However, organizing the export control regulations in the United States, especially regarding cloud computing, seems to be far from a reality.

[119] WilmerHale, *European and Transatlantic Export Controls: Europe's New Dual-Use Green Paper*, available at http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=9901 (last visited Feb 7, 2012).

[120] *Id.*

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 4, PAGE 93

Transfer of Nuclear Technology Under International Law: Case Study of Iraq, Iran and Israel

Matt Galante[1]

Citation: NAMIRA NEGM, TRANSFER OF NUCLEAR TECHNOLOGY UNDER INTERNATIONAL LAW: CASE STUDY OF IRAQ, IRAN AND ISRAEL (Martinus Nijhoff Publishers 2010).

Relevant Legal and Academic Areas: International Law; Technology Law;

Summary: The author provides an excellent summary of the international law framework guiding the safe transfer of nuclear technology for peaceful purposes between nation states. The author discusses the many benefits and uses of nuclear technology and the importance of sharing such technology throughout the world. The author focuses her legal analysis on the substantive components of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the standards outlined by the International Atomic Energy Agency (IAEA). The book ends with an examination of case studies involving the use of transferred nuclear technology in Iraq, Iran, and Israel.

INTRODUCTION

Nuclear technology has many uses beyond traditional defense-related applications. When President Eisenhower initiated the "Atoms for Peace" project in 1953, he did so with the hope that nuclear technology could be easily and safely transferred for worldwide use, while "prohibiting the spread of knowledge regarding the military uses of the atom."[2] The transfer of innovative nuclear technologies throughout the world is important because nuclear techniques can be applied in a variety of settings to revolutionize the manner in which mankind lives.[3]

---

[1] Syracuse University College of Law, Juris Doctorate Candidate 2013, Syracuse Journal of Science & Technology Law Associate Editor 2011-2012.

[2] NAMIRA NEGM, TRANSFER OF NUCLEAR TECHNOLOGY UNDER INTERNATIONAL LAW: CASE STUDY OF IRAQ, IRAN AND ISRAEL 1 (Martinus Nijhoff Publishers 2010).

[3] *Id.* at 2.

While nuclear technology can have many positive impacts on human life, it is not accessible worldwide. Typically, only developed states have the resources to advance and implement nuclear technologies.[4] It is through the use of various treaties and bilateral cooperation with developed states that developing nations gain the opportunity to access and utilize the wide array of nuclear technological advances.[5]

THE USE OF NUCLEAR TECHNOLOGY FOR PEACEFUL PURPOSES

Nuclear technology has many economically beneficial applications. First and foremost, nuclear energy can be used as a generating source of electrical power. It also has prime application in the fields of industry, agriculture, water management, medicine, pest control, crime detection, and animal breeding.[6]

In terms of animal reproduction, the viability of livestock populations is wholly dependent on optimizing animal health and improving animal reproductive performance.[7] Nuclear technology can be utilized to advance livestock productivity by analyzing parameters of livestock health, nutrition, and reproductive cycles. Nuclear and related bio-technologies can be used to study nutrient levels within the animal, the onset of puberty and sexual maturity, and the diagnosis of potentially fatal illnesses. With this information, scientists can improve livestock breeding conditions, thereby producing sustainable increases in livestock birthrates.[8] With

---

[4] NEGM, *supra* note 2 at 2.

[5] *Id.*

[6] *Id.*

[7] *Id.* at 16.

increased livestock production comes increased income generation, as livestock and livestock byproducts can be openly traded in the market for economic gains.

Pest control is a major problem worldwide, as pests can have a devastating toll on crop production and cause the spread of disease.[9] It has been suggested that pests "reduce world food production by 25% to 30%."[10] Nuclear technology can be used as an environmentally-friendly method of pest population management. Insects can be gathered into large storage areas and sterilized using ionizing radiation. Once released into nature, "the wild females are sterilized following mating with a released sterile male."[11] Nuclear technology methods are very efficient at stopping the growth of pest populations and the destruction such populations create.[12]

In the medical and human health context, nuclear technology has transformed patient treatment and the way the human body is studied.[13] Through the use of radioactive isotopes, vitamin levels can be accurately measured, and bone imaging can be conducted to search for fractures and unusual bone growth. Osteoporosis, cardiovascular disease, and a variety of genetic disorders can all be monitored through isotropic tracer detection.[14] Furthermore, nuclear medicine has become its own field of medical specialty, where doctors rely on internally

---

[8] NEGM, *supra* note 2 at 16.

[9] NEGM, *supra* note 2, at 16.

[10] *Id.* at 17.

[11] *Id.* at 16.

[12] *Id.* at 17.

[13] NEGM, *supra* note 2, at 19.

[14] *Id.*

administered open source radiation for diagnostic testing in the fields of oncology, endocrinology, neurology, cardiology, and nephrology.[15]

Many industries have used nuclear technologies to streamline production and to improve the performance, efficiency, and safety of many of their products.[16] Radiation processing is used in the manufacturing of plastics and rubbers, and has produced new materials such as hydro-dressings for the treatment of wounds.[17] Radiation is also being used to sterilize tissues, pharmaceuticals, and medical devices.[18] Radioactive isotopes are also used throughout the industry as a means of calibrating machinery, checking equipment function, and optimizing production output.

Finally, nuclear energy can be utilized to create electric power. Unlike the burning of fossil fuels, the use of nuclear energy to produce electricity does not release greenhouse gases into the atmosphere. Nuclear reactors, through a process of chain reactions during which individual atoms split, create a controlled rate of released heat. This heat is used to turn water into steam which pushes on turbine generators. This pressure forces coils of wire to interact with a magnetic field generating electric current. This current is then shipped or dispensed through power lines to customers.[19] While the majority of the world still relies on fossil fuels and hydroelectric power, advances have been made to expand the future use of nuclear power to supplement the global electricity supply.

---

[15] NEGM, *supra* note 2, at 20.

[16] *Id.* at 21.

[17] *Id.* at 21-22.

[18] *Id.* at 22.

[19] NEGM, *supra* note 2, at 23.

TRANSFER OF NUCLEAR TECHNOLOGY FOR PEACEFUL PURPOSES

As nuclear technology has many successful applications, countries around the world are striving to acquire nuclear capabilities. In 1953, President Eisenhower initiated the "Atoms for Peace" project designed to separate civilian and military use of nuclear technology. Following the project's introduction, the United Nations-sponsored Geneva Conference on the Peaceful Use of Atomic Energy established the IAEA in 1955 and created the legal framework for successfully transferring nuclear technology for peaceful purposes among nations. After it was determined that the safeguards in the IAEA were insufficient to prevent nuclear proliferation, the international community created the NPT in 1968, which was effected in 1970, and extended indefinitely in 1995.[20]

NPT GUIDELINES

Under the NPT, Nuclear Weapon States (NWS – US, Russia, UK, France, and China) are allowed to maintain their nuclear weapon capabilities. However, the goal of the treaty for these signatories was to legally prevent other countries from exploring nuclear weapon technology.[21] The NPT required bargaining and compromise. To ensure that Non-Nuclear Weapon States (NNWS) were not developing nuclear weapons, the NWS had to promise to transfer nuclear technology for peaceful purposes, provided that the receiving NNWS were kept under international supervision. The NWS also agreed to earnestly reduce their nuclear weapon arsenals over time until they were fully eliminated. The NPT works as a two-fold system: (1) it

[20] NEGM, *supra* note 2, at 41-42.

[21] *Id.* at 43.

encourages the transfer and development of nuclear technology for peaceful purposes; and (2) imposes a nuclear disarmament obligation on both NNWS and NWS.[22]

Article IV of the NPT gives signing members the authority to engage in the research, production, and development of nuclear technology for peaceful purposes.[23] It also allows for open exchange of ideas, equipment, materials, and information.[24] While Article IV encourages exchange of scientific and technological knowledge among signing members, there has been concern over the exchange of knowledge regarding "techniques relevant to enriching uranium and building power reactors."[25]

Article VI of the NPT contains the provision stipulating that parties to the treaty must undertake measures toward nuclear disarmament.[26] Since the signing of the NPT, only the US and Russia have taken progressive steps towards nuclear disarmament, though their pace has been extremely slow.[27] France, UK, and China have not undertaken any means to limit their development of nuclear weapons in compliance with Article VI.[28] The indefinite extension of the NPT in 1995 has given NWS indefinite time to start their decrease in nuclear arsenals,

---

[22] NEGM, *supra* note 2, at 43.

[23] *Id.* at 45.

[24] *Id.*

[25] *Id.* at 48.

[26] NEGM, *supra* note 2, at 52.

[27] *Id.* at 53.

[28] *Id.*

thereby rendering Article VI unenforceable and eliminating a definite time frame under which NWS must eliminate nuclear weapon capabilities.[29]

The NPT has many inadequacies including the treaty's discrimination between NWS and NNWS and the failure of NWS to begin meeting their obligations under the Article VI disarmament provisions. The current rules lack the force needed to ensure the elimination of all nuclear weapons worldwide. Moreover, as global terrorist organizations gain more power and support, the threat of nuclear proliferation and the use of such weaponry remains a viable threat.[30]

IAEA RULES

The IAEA was established as an autonomous organization in 1957 with the goal of promoting "peaceful uses of nuclear energy for the benefit of humanity."[31] The IAEA ensures that nuclear projects conducted by member states remain peaceful in nature. After the signing of the NPT in 1970, the IAEA is responsible for ensuring the NPT NNWS signatories comply with the nonproliferation requirements of the treaty.[32] Under Article II of the IAEA statute, the organization is tasked with two objectives: (1) to accelerate the spread and use of atomic technology for "peace, health, and prosperity throughout the world;" and (2) to ensure that such technology is not used for "any military purpose."[33]

---

[29] NEGM, *supra* note 2, at 55.

[30] *Id.* at 59.

[31] *Id.* at 61.

[32] *Id.*

[33] NEGM, *supra* note 2, at 61.

Additionally, the IAEA provides scientific and technical assistance to member states during nuclear projects and administers established safeguards to guarantee that projects using nuclear technology are not being manufactured for defense and military purposes.[34] Article III of the NPT obliges NNWS to accept IAEA safeguards regarding the use of nuclear technology.[35] These safeguards give the IAEA authority to conduct investigations and inspections of NNWS nuclear projects to ensure that such projects are not enriching uranium for military purposes.

The IAEA utilizes two safeguard systems while inspecting nuclear projects. Before the NPT began in 1970, the IAEA would conduct investigations on an independent case-by-case basis upon the request of either the supplying or receiving state. This process is still used for non-NPT members.[36] The second safeguard system is found in Article III of the NPT, which requires NNWS to accept all IAEA safeguards. NNWS must report all nuclear activities to the IAEA and the Agency has the right of access to conduct investigative inspections to ensure all nuclear activities remain peaceful.[37] The IAEA has the authority to conduct three types of inspections: (1) routine inspections, (2) ad hoc inspections, and (3) special inspections.[38] Before the IAEA can undertake special inspections, the Director General of the IAEA must determine that there is reasonable evidence for suspecting illegal nuclear proliferation. Any state under the NPT not participating in illegal nuclear activities would likely grant inspectors access to dispel

---

[34] NEGM, *supra* note 2, at 61.

[35] *Id.*

[36] *Id.* at 5, 63.

[37] *Id.* at 68.

[38] NEGM, *supra* note 2, at 68.

suspicion. However, any state violating NPT obligations would deny IAEA inspector's access to their facilities. Such behavior would qualify as reasonable suspicion that the state is trying to conceal treaty violations and uranium enrichment.[39]

The IAEA has legal authority to search for nuclear weapon programs, yet the safeguards still require modification to ensure the goals of the IAEA are achieved. This is evidenced by the failure of the IAEA to identify the presence of the covert Iraqi nuclear program in the 1990s.[40] While the IAEA has taken steps to ensure quality of its inspections, the Agency is still required to rely on the cooperation of NNWS, as the rules do not place obligations on supplying states. These rules limit the Agency's capability of assessing illegal nuclear activities.[41]

CASE I: IRAQ

Although a member to the NPT and IAEA, Iraq had initiated an active covert nuclear program designed to enrich uranium in violation of its international non-proliferation obligations. Iraq began developing its own nuclear technology in the 1950s with the creation of small mega-watt reactors.[42] During the 1970s, Iraq began dispatching Iraqi scientists to train in nuclear technologies around the world. At that time, Iraq also began to invest extensive financial resources into its nuclear program. The immediate goal of the program was to secure nuclear technology with long term objectives of creating nuclear weapons. With the secret operations underway, Iraq was hosting IAEA inspectors in its declared facilities in cooperation with its NPT

[39] NEGM, *supra* note 2, at 71.

[40] *Id.* at 78.

[41] *Id.*

[42] *Id.* at 148.

obligations.[43] In 1974, Iraq dispatched an Iraqi "scientist attaché" to its Vienna Embassy with the sole objective of working with the IAEA. Iraq used the information it obtained from the diplomat as a means to cover up its illegal nuclear activities.

In the late 1970s, Iraq began to contract with various countries and businesses to purchase materials necessary for the enrichment of uranium.[44] To avoid export regulations, Iraq would divide equipment orders into sub-components and employ the use of intermediaries to hide purchases. It was not until 1991 that the IAEA discovered "the scope and intensity of the Iraqi nuclear weapons program."[45] It was determined that Iraq's nuclear program was dependent on external supplies provided by many international suppliers including Germany, UK, Switzerland, US, Austria, Yugoslavia, Japan, Italy, Brazil, and Niger.[46] Iraq's actions violated Articles II and III of the NPT.

During the 1970s, Iraq's nuclear developments were in line with the NPT protocols, as its actions were in pursuit of peaceful nuclear technology. However, in subsequent years, the concentration and goals of the nuclear projects were shifted to the development of nuclear weapons, and Iraq's clandestine approach to this goal constituted direct violation of the NPT and the safeguards established under the IAEA.[47]

---

[43] NEGM, *supra* note 2, at 148.

[44] *Id.* at 149.

[45] *Id.* at 151.

[46] *See id.* at 152-59.

[47] *See* NEGM, *supra* note 2, at 160-62.

Iraq was the first country to violate the NPT. Since 1991, the United Nations Security Council (UNSC) has adopted several resolutions to disarm Iraq's nuclear capabilities.[48] In creating its weapons program, Iraq deceived both the IAEA and the international firms that provided its much needed supplies. The episode in Iraq displayed the IAEA's inadequacy in successfully inspecting countries for nuclear weapons programs, and the failure of the IAEA to use a cohesive process and modern technology to assist in its inspection duties.[49]

CASE II: IRAN

While IAEA findings indicate the Iranian nuclear program is directed towards peaceful purposes, several States believe Iran is covertly investigating military uses for nuclear energy.[50] Iran became a member of the NPT when it ratified the treaty in 1970.[51] In the early 1970s, Iran announced a long-term endeavor to develop nuclear power plants for electric power. Thus far, Iran has fulfilled almost all of its obligations under the NPT.[52] However, the IAEA has discovered that in recent years, Iran neglected to report all information regarding its nuclear program to the IAEA for review.[53]

Before 2002, Iran had been in compliance with all treaty obligations, but in 2002 Iran failed to report to the IAEA the import of fissionable material and neglected to follow IAEA

---

[48] NEGM, *supra* note 2, at 183.

[49] *See id.* at 185-86.

[50] *Id.* at 8.

[51] *Id.* at 193.

[52] NEGM, *supra* note 2, at 193.

[53] *Id.* at 194.

prescribed safeguards.[54] It was later determined that Iran also concealed information regarding the capabilities of some of its nuclear facilities.[55] To mend this breach, IAEA inspection teams conducted extensive inspections to ensure Iran was compliant with its NPT obligations.[56] Even with the concern from western nations over Iran's nuclear activities, Iran has accepted IAEA safeguards and has declared that all nuclear activities are being conducted for peaceful purposes.

CASE III: ISRAEL

The case study on Israel is unique because Israel is not a member to the NPT and only a limited number of its nuclear facilities fall under IAEA safeguards.[57] Since the birth of the Israeli state in 1948, the country has been actively engaged in nuclear research for both military and peaceful purposes.[58] President Eisenhower's "Atoms for Peace" project in 1955 provided Israel with nuclear training and helped fund and construct a 5 mega-watt nuclear reactor for Israel.[59] However, it was Israel's relationship with France that led to its acquisition of nuclear bombs. Israeli scientists trained at the French Sarclay Institute in the art of nuclear reactions. The scientists participated in the production of a small reactor powered by uranium and heavy water. Once back in Israel, the scientists built a similar reactor powered by indigenous uranium

[54] NEGM, *supra* note 2, at 195.

[55] *Id.* at 197.

[56] *Id.* at 194.

[57] *Id.* at 227.

[58] NEGM, *supra* note 2, at 227.

[59] *Id.*

and locally available heavy water.[60] In the late 1950s, the French supplied Israel with a plutonium reactor in Dimona. American spy planes noted subterranean digging in Dimona and concluded that Israel was creating a nuclear weapon.[61] By June 1967, Israel had completed its weapons design and was capable of manufacturing warhead missiles.[62] Israel has stated that they will only use their nuclear weaponry in response to actual attacks on Israel, and will not use them as a pre-emptive tool against suspected aggression.[63]

Israel has refused to join the NPT because "in the absence of reliable arrangements for preventing armed conflict, nuclear deterrence is essential for the survival of the nation."[64] Even though Israel is not a member of the NPT, it is a member of the United Nations Charter and has legal obligations to adhere to resolutions by both the UNSC and the United Nations General Assembly.[65] UNSC Resolution 487 of 1981 requested Israel "adhere to the NPT and to place its nuclear facilities under full scope safeguards."[66] Furthermore, the Israeli nuclear program has been a subject of annual General Assembly regulations, some specifically urging the country to place its nuclear facilities under IAEA safeguards.[67] Thus, Israel is in direct conflict with its responsibilities under the United Nations Charter.[68]

---

[60] NEGM, *supra* note 2, at 229.

[61] *Id.*

[62] *Id.* at 230.

[63] *Id.* at 232.

[64] NEGM, *supra* note 2, at 241.

[65] *Id.* at 257.

[66] *Id.* at 243.

[67] *Id.* at 247.

CONCLUSION

The use of nuclear technology has been one of the most contentious debates throughout history. Many proponents laud nuclear power as a sustainable form of energy that can reduce carbon emissions and increase global energy security. Opponents argue that the use of nuclear power creates many threats to human health and the environment, including the health risks associated with uranium exposure, environmental damage from uranium mining, the problem of disposing radioactive nuclear waste, and the potential for nuclear weapons proliferation. Throughout this book, Ms. Negm thoughtfully explains the controversies that surround the global nuclear regulatory schemes and their applications in countries that have been notorious for their use and transfer of nuclear technology.

---

[68] NEGM, *supra* note 2, at 257.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 5, PAGE 107

Reframing Rights: Bioconstitutionalism in the Genetic Age

Brianne Yantz*

Citation: SHEILA JASANOFF ET AL., REFRAMING RIGHTS: BIOCONSTITUTIONALISM IN THE GENETIC AGE (Sheila Jasanoff ed., 2011).

Relevant Legal and Academic Areas: Biological and Life Sciences, Biotechnology, Medical Ethics, and Law

Summary: *Reframing Rights: Bioconstitutionalism in the Genetic Age* assesses the evolving relationship between science and the law. Specifically, the authors focus on how advances in biological sciences and biotechnology in the last century have promulgated changes regarding the legal conception of life and individual rights. Told through a series of case studies, *Reframing Rights* argues these changes in law and science should be considered "bioconstitutional." Topics such as sterilization, DNA testing, and xenotransplantation are among those examined and argued by the authors as demonstrative of constitutionally significant changes that have developed between individuals, science, and the state in recent decades. With such considerable changes, the authors contend, the law must constantly evolve to maintain the balance between individual rights and state authority.

I. Introduction

In *Reframing Rights: Bioconstitutionalism in the Genetic Age*, the focus of the authors' inquiry is on the intersection between biosciences and the law in recent decades. The book's primary author and editor, Sheila Jasanoff, presents the argument that scientific and legal scholarship are not completely separate and conflicting studies. Rather, a great deal of influence and overlap exists between the two, particularly in the emerging fields of biology and biotechnology.[1] With this in mind, Jasanoff and her co-authors propose greater study into the

* Syracuse University College of Law, Juris Doctorate Candidate 2013, Syracuse Journal of Science & Technology Law Associate Editor 2010-2011.

[1] SHEILA JASANOFF ET AL., REFRAMING RIGHTS: BIOCONSTITUTIONALISM IN THE GENETIC AGE 1-5 (Sheila Jasanoff ed., 2011).

areas of convergence between science and the law, which they refer to as "bioconstitutionalism"; furthermore, they advocate for legal reforms that properly account for the impact of biosciences and biotechnology on individual rights.[2]

To illustrate the book's arguments, Jasanoff and her colleagues explore how different areas of biological or biotechnological focus currently relate to the law and explain why there is a need for change. Accordingly, this review seeks to examine the authors' assessments. Specifically, the following topics will be addressed: first, a case study involving sterilization practices in California; second, the concept of biopolitics, or the power to govern life, in embryonic stem-cell research and cloning; third, the role of DNA and other forensic technologies in the criminal justice system; fourth, concerns regarding human health in xenotransplantation and the imaginative concept of Genomic Health; and fifth, how the relationship between the people and their governments demonstrates the need for a reformation of legal principles. Once each topic has been discussed, this review will also highlight the significance of the authors' analyses and present a clear assessment of the book's argument.

II. Case Study: Sterilization

In the first area of assessment, co-author Alex Wellerstein delves into the intersection of law and biotechnology by examining the practice of sterilization. Specifically, he focuses his study on the state of California and its institutions for the mentally ill, which had produced the largest number of sterilized patients in the first half of the twentieth century.[3] However, the

---

[2] *See* JASANOFF ET AL., *supra* note 1, at 4-5.

[3] *Id.* at 29.

purpose of Wellerstein's inquiry is to prove, as he hypothesizes, that the record number of sterilizations within California during this period were not solely driven by the popular social ideology of eugenics, which he defines as "the desire to improve the human gene pool by discouraging the reproduction of the 'unfit.'"[4] Rather, Wellerstein argues that the legal power to sterilize, and how it had snaked its way through California's local medical and social infrastructures, was primarily to blame for the state's egregious record.[5]

As there was no federal statute regarding sterilization practices in the early nineteen hundreds, such laws fell to the hands of the states.[6] Originally enacted in 1909, California's state statute was amended by the legislature on various occasions, and the result was a law that permitted sterilization for a wide variety of reasons.[7] The law also granted hospital physicians, administrators, and superintendents a broad amount of discretion in determining if an individual should be sterilized, and did not require a specific explanation be given.[8] According to Wellerstein, it was evident that the personal beliefs and ideologies of these authority figures easily controlled the decisions about which patients required sterilization.[9] Thus, it was the inadequacies of the state law that had allowed for this "unchecked authority" to promote this eugenics-like practice.[10]

---

[4] JASANOFF ET AL., *supra* note 1, at 29-30.

[5] *Id.* at 30.

[6] *Id.* at 32.

[7] *Id.* at 31-36.

[8] JASANOFF ET AL., *supra* note 1, at 35.

[9] *See id.* at 42-44.

[10] *See id.* at 53.

Such a discovery is important to the discussion of bioconstitutionalism because sterilization is a popular focus of historical study that demonstrates how the intersection of the biological sciences with the law has instigated social change.[11] Moreover, what is evident from this discussion is that social progress mandates that the interdependent relationship between the law and science be realized. With this in mind, the authors move into a more general discussion regarding the government's power to govern life.

III. The Power to Govern Life

The discussion next moves into the realm of biopolitics, a term coined by French social theorist Michel Foucault, which concerns the government's power to govern life.[12] One specific area of focus is the ethical and legal battles that have surrounded embryonic stem-cell research.[13] According to Jasanoff, the cultural beliefs and ethics of a nation are highly determinative in the substance of the laws that govern this field of research.[14] For this reason, it has been difficult for lawmakers to define the legal status of an embryo. While different nations have settled on different determinations, the United States has been particularly indecisive for a long time.[15] However, through bioethics, certain facets of life have been scientifically defined, which has given the United States the necessary justifications for evoking certain legal parameters.[16]

[11] JASANOFF ET AL., *supra* note 1, at 31.

[12] *Id.* at 59.

[13] *Id.* at 62-64.

[14] *Id.* at 61.

[15] JASANOFF ET AL., *supra* note 1, at 67.

[16] *See id.* at 77-79.

To contrast this, co-author Ingrid Metzler addresses in a later chapter the law in Italy, which has barred 'scientists from "killing" Italian embryos for stem cell procurement.'[17] Such a restriction, she contends, signifies the oppression of the state on the biosciences, which also inhibits the rights of the people.[18] These political contrasts legitimize the idea of bioconstituionalism. Further, it is evident from this discussion that without such a framework for rights, hegemonic forces within a nation could easily be able to overtly and oppressively control the people by limiting their abilities to research and implement medical practices that could be lifesaving.

In the next area of discussion, the authors focus on the practice of cloning. Specifically, co-author Guiseppe Testa examines how the law enabled cloning practices in Britain, Italy, and the United States to be recognized as socially legitimate.[19] Testa seeks to investigate how each nation defines the term "clone," as well as their respective policies concerning the practice of cloning.[20] What is discovered is that the definitions of natural and artificial have varied among nations, which highlights how political cultures are integral to the development of biosciences.[21] However, of greater importance is that, despite these differences, each nation has demonstrated the need to articulate the public purpose of these developments in cloning, which imposes upon the law the duty to legitimatize its existence.[22] Thus, it is evident through this assessment of

[17] JASANOFF ET AL., *supra* note 1, at 106.

[18] *See id.* at 106-107.

[19] *Id.* at 85.

[20] *Id.* at 86.

[21] JASANOFF ET AL., *supra* note 1, at 102.

[22] *Id.*

cloning, as well as embryonic stem-cell research, that there is an inevitable crossover between the biosciences and the law, which the authors would argue requires a constitutional reformation of individual rights. Further, as the authors seem to suggest, without such recognition of rights, the government may have the unlimited power to govern life.

IV. Modern Technology and the Criminal Justice System

The next concept addressed by the authors is the role of technology in the modern criminal justice system. First, co-author Jay D. Aronson addresses the issue of postconviction DNA testing and constitutional rights.[23] Aronson explains that new advances in "forensic DNA analysis is increasingly being used in postconviction litigation to prove that innocent people have been wrongfully incarcerated."[24] Yet, at the core of Aronson's assessment are the notions of finality and certainty; in the United States, he explains, an individual can be incarcerated as long as his constitutional rights have not been violated, which demonstrates a preference for finality in legal proceedings rather than certainty of guilt.[25] Because there is no fundamental right to DNA testing, the law has been heavily criticized; however, most states as well as the federal government have mandated testing in certain situations through legislation.[26] Still, the laws vary from state to state, meaning there is no "ironclad" guarantee of postconviction DNA testing.[27]

[23] *See* JASANOFF ET AL., *supra* note 1, at 125.

[24] *Id.* at 126.

[25] *See id.* at 125-28, 142.

[26] *Id.* at 126.

[27] JASANOFF ET AL., *supra* note 1, at 127.

For this reason, there is an argument for the expansion of rights that accounts for the possible remedies afforded by technological advancement.[28]

Whether these rights should be fundamental is highly debated because DNA testing is not infallible and would not necessarily advance justice if it were to be treated as foolproof.[29] The flipside to that argument is that strong evidence of innocence does not have to be perfect – any cause for reasonable doubt would be sufficient.[30] Through this debate, the growing concern for individual rights is again evident; the law in its current stage would prefer finality for public face rather than certainty of guilt before stripping the individual of his rights. Because of the inadequacies of the law in protecting individual liberties, a compelling argument for bioconstitutionalism and the rectification of rights is apparent.

Following Aronson's discussion of DNA testing, co-author David E. Winickoff next addresses DNA databases, which are "reshaping legal understandings of security, freedom, and identity."[31] Modern technologies such as the Combined DNA Index System (CODIS), a network that allows federal, state, and local crime labs to electronically exchange DNA profiles, have permitted more thorough and efficient criminal investigations.[32] The concern here, however, is whether technology has gone too far in breaching personal privacy, albeit through largely virtual

[28] *See* JASANOFF ET AL., *supra* note 1, at 127-28.

[29] *Id.* at 141.

[30] *Id.* at 141-42.

[31] *Id.* at 147.

[32] *See* JASANOFF ET AL., *supra* note 1, at 148.

means.[33] Specifically, it has been argued that government use of new and invasive forensic technologies, such as a DNA database, is a violation of the Fourth Amendment,[34] which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things seized.[35]

From the text of the Fourth Amendment, it is evident the concern with the DNA database is that it may constitute an unreasonable search or seizure of one's private genetic material, depending on the context in which the database is used.[36] Despite these concerns, judges have continually disagreed over whether DNA databases even require a Fourth Amendment analysis;[37] thus, as of yet, there is no clear and accepted argument that DNA databases delve too far into personal privacy as to violate ones constitutional rights.

Currently, judges have discretion in determining on an individual case basis the constitutionality of government forensic inquiry and whether there has been a violation of rights.[38] Again, there are competing approaches to the current legal framework; one faction argues that DNA databases and similar forensic technologies are a "lurking dystopia," while others advocate for continued leniency and discretion because of the greater need for public safety.[39] Regardless of varying judicial interpretations, one thing is clear: these new

---

[33] *See* JASANOFF ET AL., *supra* note 1, at 147-49.

[34] *Id.* at 148.

[35] U.S. CONST. amend. IV.

[36] *See* JASANOFF ET AL., *supra* note 1 at 149.

[37] *Id*. at 151.

[38] *See id.* at 164-65.

[39] *See id.* at 165.

biotechnologies will continue to bring about changes that will require the government to constantly reassess its laws to ensure the rights of the people are not violated.

From these discussions, it is clear that technological advancements have greatly impacted the criminal justice system in recent decades. As both Aronson and Winickoff point out, there is great concern for how the law currently addresses these changes. Although, in the case of DNA databases, most judges have yet to find individual rights infringed upon to the point that such an intrusion is a constitutional violation, it is clear why there is reason for concern. Furthermore, it is evident that a reassessment of individual rights and their protections, particularly under the U.S. Constitution, will become increasingly necessary as biotechnologies allow greater access into people's private lives, so that the criminal justice system can operate as a stable institution that guarantees the protection of individual liberty. From these discussions of the criminal justice system, the authors next look at health care.

V. Biotechnology and Human Health

The next topic of discussion concerns biotechnologies and health care. First, co-author Mariachiara Tallacchini addresses xenotransplantation, which is "the transplant of cells, tissues, or organs between different species."[40] According to Tallacchini, experiments in xenotransplantation began around the 1960s.[41] However, it was not until 1984 that the general public became aware of such experiments – in that year, "Baby Fae," the infant that survived twenty-one days after she was given a baboon heart, made headlines.[42] In earlier years, the

[40] JASANOFF ET AL., *supra* note 1, at 169.

[41] *Id.* at 171.

[42] *Id.*

practice was highly controversial and arguments against xenotransplantation generally revolved around the ethical treatment of animals.[43] There was also a wealth of concerns for individual rights, particularly that of informed consent, because the little known effects posed enormous health risks.[44]

In the United States, xenotransplantation at its infancy was a cause for major public anxiety; the potential for spreading infections, such as AIDS, through the practice was initially very high.[45] Yet, despite all the concern, xenotransplantation has become an accepted practice throughout the world – primarily because the law has reshaped and resized the risks involved to "resemble ordinary forms of risk." [46] Thus, xenotransplantation now serves as a model for how legal changes have accommodated scientific advancements while preserving the integrity of individual and collective rights. Through regulatory orders implemented in nations across the globe, the practice of xenotransplantation has become much safer.[47]

Following the discussion of xenotransplantation, co-author Kaushik Sunder Rajan addresses a concept called Genomic Health.[48] The appeal of Genomic Health is freedom of choice; using an individual's genomes, accurate assessments could be made involving individual health risks that would ultimately minimize a person's particular health risk through preventative

---

[43] JASANOFF ET AL., *supra* note 1, at 169-70.

[44] *Id.* at 170.

[45] *Id.* at 173-77.

[46] *See id.* at 188.

[47] JASANOFF ET AL., *supra* note 1, at 188.

[48] *Id.* at 198.

measures.[49] Currently, such an imaginative and experimental idea has little legal support within the United States.[50] However, it is clear that Rajan advocates for further inquiry into this line of health care, as well as a possible reworking of the law to allow for its implementation, as the benefits would be enormous.

Clearly, the authors' discussions of biosciences and biotechnology as they relate to health care have unearthed ways in which the law has made once dangerous and experimental methods of treatment safer. At the same time, these discussions have also addressed ways in which the law has yet to consider current experimental methods of research and treatment. This contrast shows that lawmakers have made some strides to improve healthcare as new technologies evolve, but can in some instances be unwilling or unable to act. After an exhaustive discussion of health care, the authors' next take a deeper look into the relationship between the people and their governments.

VI. Between Citizens and Their Governments

After careful analysis of specific advancements within the biosciences, co-authors Robert Doubleday and Brian Wynne address the relationship between citizens and their governments; specifically, they examine public engagement in the sciences and the place of the people in shaping public knowledge.[51] Utilizing the United Kingdom as the focus of study, Doubleday and Wynne examine how much control citizens have over policy choices regarding

[49] JASANOFF ET AL., *supra* note 1, at 198-202.

[50] *Id.* at 212.

[51] *Id.* at 241.

biotechnologies.[52] According to the authors' assertions, it appears the British government, with its own scientific agenda, has been undermining the legitimacy of the public and the agency of individual citizens.[53] As Doubleday and Wynne highlight, "[i]n effect, citizens play a role on [the] condition of alignment of their meanings with those already laid down by science and the state."[54] If true, this assertion further supports the need for a reframing of rights worldwide that address the changes in law and society brought on by the biosciences.

Another point of contention for the authors is the reordering of society that has appeared in recent decades: while genetic understandings of human life have emerged, it has become evident that the "legal and social meanings" are in no way transparent.[55] Science has become a necessity in society, largely because of the commercial markets and the concept of consumerism; yet the social, political, and economic ramifications of advancement are still unclear.[56] Thus, co-author Jim Drawta's discussion of the "precautionary principle," which has been implemented throughout Europe is of important note. Although the United States is skeptical about this principle, it is important because it deals with "the scientific uncertainties surrounding the regulation of biotechnology."[57] Drawta advocates that the precautionary principle is essential because, in factoring risk and predictability, it serves as a legitimate means of regulating the

[52] *See* JASANOFF ET AL., *supra* note 1, at 241.

[53] *Id.*

[54] *Id.*

[55] *Id.* at 3, 256.

[56] *See* JASANOFF ET AL., *supra* note 1, at 263, 281-83.

[57] *Id.* at 263.

biosciences and how they interact with individuals and institutions.[58] Furthermore, Drawta alleges that, as a careful legal approach to biotechnology, it has distinctive strengths that serve the constitutional needs of the people.[59] The accuracy of his assertion is evident from the successful use of the precautionary principle in Europe.[60]

Although Drawta provides good reason to suggest the need for the precautionary principle in America, it appears that such a method is just one way to approach the growing relationship between biotechnology and the law. Moreover, the more important message is that advances in biosciences require a profound rethinking of individual rights. Essentially, Drawta's discussion leaves the reader with the stark realization that, in order for society to advance, the law needs to seriously consider how the biosciences affect the freedoms and safeties of the people.

VII. Conclusion

As evidenced by the topics of discussion throughout, it is clear that the book's objective is to address the more significant biological and technological changes in recent decades and demonstrate how they fit into the framework of bioconstitutionalism. Each of the areas assessed strengthen the foundation of the book's central argument, with the first object of observation laying the corner stone. Wellerstein's examination of the sterilization practices in California exemplifies how the lack of a uniform set of constitutional protections allowed for authority figures to abuse power and make decision based upon personal convictions rather than law.

---

[58] *See* JASANOFF ET AL., *supra* note 1, at 263-64.

[59] *See id.*

[60] *See id.* at 281-83.

Moving away from the historically popular mode of inquiry, the second area of assessment, regarding embryonic stem-cell research and cloning, addresses a similar concern: the power of the government or other elite political entities to govern life. The following third subject of study highlights how the lack of a "bioconstitutional" framework has allowed the government to exercise, and perhaps abuse, its discretion in utilizing forensic technologies to advance the criminal justice system. The fourth issue of inquiry, the concerns regarding human health in xenotransplantation and the concept of Genomic Health, serves to contrast the government's willingness and abilities to provide proper legal accommodations for emerging technologies regarding human health. While the law has the reduced risk factors involved with experimental technologies involving interspecies organ transplants, it currently fails to support a project that could prove significantly beneficial to the medical field. Lastly, the fifth entity of examination, the relationship between the people and their governments, serves to tie the book's central argument, advocating for a constitutional reformation of rights, back together.

As exemplified by the various topics addressed, it is evident throughout the book that the authors' advocacy for bioconstitutionalism stems from a deeply rooted concern for the preservation and future protection of individual rights. Such freedoms, the authors contend, are very much in danger if the framework of the Constitution fails to keep up with changes in science. In presenting this argument, the authors clearly identify how key technological and scientific innovations of recent decades have affected individual rights and present realistic insight as to what the future may hold. Accordingly, this leaves the reader with the disconcerting realization that a reformation of constitutional rights is necessary to adequately prepare individuals and institutions for a society inescapably linked to biosciences and technologies.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 28 SPRING 2013 ARTICLE 6, PAGE 121

The Evolution of E-Discovery Model Orders

Daniel B. Garrie, Esq. and Candice M. Lang, Esq.

Abstract

This article analyzes the Federal Circuit's Model Order regarding E-Discovery in patent cases (the "Model Order"). The article (i) briefly describes the purpose behind the Model Order, (ii) describes its key provisions, and then (iii) analyzes the Model Order to identify some areas of continuing concern. The authors conclude that, while it is beyond refute that the Model Order is a step in the right direction in the courts' efforts to control and manage e-discovery, the Model Order is only a first step. In this regard, several problems, as set forth below, can potentially arise when counsel or the courts use the Model Order. It is hoped that this article will encourage judges, litigants, and other interested parties to continue trying to solve some of the still troubling aspects of e-discovery and e-discovery abuse.

Table of Contents

I. THE MODEL ORDER: AN ATTEMPT TO CONTROL AND MANAGE E-DISCOVERY…. 123

II. A REVIEW OF THE KEY PROVISIONS OF THE MODEL ORDER…… 124

III. THE MODEL ORDER: AREAS OF CONTINUING CONCERN…… 125

A. The Model Order's Triggers for Cost Shifting Allow the Parties to Game the System and May Offer Disincentives to More Economical Alternatives in E-Discovery……126

B. The Model Order Default Standard that Metadata Is Not To Be Produced Absent a Showing of Good Cause Ignores the Critical Value Metadata Provides When Issues Exist Around Authenticity or Authorship..……127

C. The Model Order Only Allows Email Production to Occur After the Parties Have Exchange Initial Disclosures of Basic Documents and Information on the Critical Systems Storing the Email. ……. 127

D. The Model Order Should Consider Requiring the Parties to Perform Email Sampling Before Limiting the Number of Search Terms and Custodians to Five People and Terms. ……. 129

IV. CONCLUSION…… 130

The E-Discovery Dance for Patent Litigation: The Federal Circuit Tries to Change the Tune

Daniel B. Garrie, Esq. and Candice M. Lang, Esq.[1]

I. THE MODEL ORDER: AN ATTEMPT TO CONTROL AND MANAGE E-DISCOVERY

The Model Order Regarding E-Discovery in Patent Cases (the "Model Order")[2] is the Federal Circuit's response to the exponential growth of e-discovery and related costs in cases before it.[3] As noted in the Introduction to the Model Order, patent cases tend to suffer from disproportionally high discovery expenses—with one study determining that the costs of an intellectual property case run almost 62% higher than other litigations.[4] Moreover, the exponential growth in electronic documents and communications has, intentionally or otherwise, led to what the Federal Circuit considers to be excessive e-discovery.[5] Broad and unfettered e-discovery—particularly email related discovery—has led to litigations where the time and cost of electronic production far outweighed the minimal benefits of marginal and cumulative disclosure, thus threatening to derail the judicial promise of just, speedy and affordable determination of disputes:

---

[1] Daniel B. Garrie, Esq. is a partner at Law & Forensics, splitting his time between the East and West coast offices where he focuses on forensics, e-discovery, cyber security, and related investigations, including in the area of intellectual property disputes. Mr. Garrie can be reached at daniel@lawandforensics.com. Candice M. Lang, Esq. is Associate Counsel in the New York office of Law & Forensics, where she concentrates her practice on digital forensic investigations, e-discovery, and cyber security. Ms. Lang can be reached at clang@lawandforensics.com. The views expressed herein are solely those of the authors.

[2] E-Discovery Model Order, *available at* http://memberconnections.com/olc/filelib/LVFC/cpages/9008/Library/Ediscovery%20Model%20Order.pdf.

[3] *See supra* note 2 at 2.

[4] *See id.* at 1 (citing Emery G. Lee III & Thomas E. Willging, *Litigation Costs in Civil Cases: Multivariate Analysis* 8 (Fed. Judicial Ctr. 2010)).

[5] *Id.* at 2.

> As technology and knowledge play an increasingly important role in our economy, the courts must not become an intolerably expensive way to resolve patent disputes. Specifically, litigation costs should not be permitted to unduly interfere with the availability of the court to those who seek to vindicate their patent rights—the enforcement of such rights is both an obligation of the legal system and important to innovation. Likewise, disproportionate expense should not be permitted to force those accused of infringement to acquiesce to non-meritorious claims.[6]

The Model Order provides the courts and counsel with a framework for managing the e-discovery process and the responsible, targeted use of e-discovery in patent cases. It seeks to "promote economic and judicial efficiency by streamlining e-discovery, particularly email production, and requiring litigants to focus on the proper purpose of discovery—the gathering of material information."[7]

II. A REVIEW OF THE KEY PROVISIONS OF THE MODEL ORDER

The Model Order attempts to get both parties to engage in targeted e-discovery by placing presumptive limits on e-discovery. In this regard, the Model Order has patterned itself after Federal Rule of Civil Procedure 30, which limited deposition practice by presumptively limiting each side to ten depositions of seven hours each.[8] Specifically, the Model Order requires the parties exchange the type of core documentation key to every patent litigation – *i.e.*, documents concerning (i) the patent; (ii) the accused product; (iii) the prior art; and (iv) the relevant finances – before propounding email requests.[9] Even then, the Model Order

---

[6] E-Discovery Model Order, *supra* note 2, at 2.

[7] *Id.* at ¶ 1 ("This Order . . . streamlines Electronically Stored Information ("ESI") production to promote a 'just, speedy, and inexpensive determination' of this action").

[8] *Id.* at 3; FED. R. CIV. P. 30.

[9] E-Discovery Model Order, *supra* note 2, at ¶ 8.

presumptively limits the number of custodians and search terms for all email production requests, so that any email production requests are focused on particular issues and areas for which email discovery is appropriate.[10] These limits are presumptive only, and may be modified by the parties or the court for good cause shown.[11]

Where a party seeks more discovery than agreed upon by the parties, or allowed by the court, the requesting party bears the reasonable cost of that discovery.[12] By shifting costs, the Model Order seeks to ensure that a party carefully balances the cost and value of the additional discovery.[13]

The Model Order also seeks to lower the cost of e-discovery by addressing a large source of that cost – pre-production review of documents by attorneys or other human reviewers. To minimize such pre-production review, the Model Order expressly provides that the inadvertent production of attorney-client privileged or work product documents during e-discovery may not be used in the pending case, and does not constitute a waiver in the pending case, in any other federal or state proceeding, or for any purpose.[14]

III. The Model Order: Areas of Continuing Concern

The Model Order is a good first step at addressing the major problem with e-discovery: its ever-increasing complexity, cost and expense. However, the solutions provided by the Model Order raise several concerns, four of which are identified and discussed below.

---

[10] E-Discovery Model Order, *supra* note 2, at ¶¶ 6, 7, 10, 11.

[11] *Id.* at ¶ 2.

[12] *Id.* at ¶¶ 10, 11.

[13] *Id.* at 3-4.

[14] E-Discovery Model Order, *supra* note 2, at ¶¶ 12-14.

A. The Model Order's Triggers for Cost Shifting Allow the Parties to Game the System and May Offer Disincentives to More Economical Alternatives in E-Discovery

The first potential area of concern with regards to the Model Order arises from the Model Order's reliance on disproportionate costs to trigger cost shifting.[15] In this regard, it is possible for counsel for the producing party to manipulate the discovery process so as to increase costs and force the requesting party to bear those costs. Specifically, the costs of performing data collection or execution can sometimes be substantially less costly if done in-house, than if a third-party vendor collected and performed the search.

For example, a large technology firm might have a proprietary document tracking platform that runs on legacy hardware, and an in-house IT team that is familiar with and manages this system. In such cases, it would be substantially more costly to retain a third-party vendor, than to use the in-house IT department. Yet, that expense arguably could still be presented to the court and opposing counsel as a true cost in e-discovery, and be used to deter, narrow, or shift the costs of e-discovery. Indeed, the producing party can contend that using a third-party vendor is appropriate, because doing so will avoid any concern that in-house IT staff will inevitably skew the production results in favor of the producing party. The end result is that a party can, or at least can try, to intentionally trigger cost shifting as a tactic in litigation.

Courts and litigants should be aware of this tactic, and raise the issue during the initial discovery conference mandated by Federal Rule of Civil Procedure 26. One solution is for the courts to encourage parties to utilize their own IT departments when possible to collect and

[15] E-Discovery Model Order, *supra* note 2, at ¶ 3. The Model Order also provides that discovery tactics that delay or prolong the process will be considered by the Court in determining which party should bear the costs of the discovery process.

produce documents, as long as best practices are followed by the in-house IT department in collecting and producing those documents.

B. The Model Order Default Standard that Metadata Is Not To Be Produced Absent a Showing Of Good Cause Ignores the Critical Value Metadata Provides When Issues Exist Around Authenticity or Authorship

The second area of concern with the Model Order is its default standard of no metadata (*i.e.*, "data about data") absent a showing of good cause.[16] In a segment of patent related disputes that focus on the date of filing, on priority, or on who is the creator of a patent, metadata is likely to be a critical element that provides crucial information regarding such key points as dates, times, authorship, and other related elements.[17] Although, the Model Order does allow parties to request metadata upon a showing of "good cause", it is an uphill effort for counsel to establish "good cause" around metadata because even after the initial discovery conference, litigants may not have enough information to determine specifically what metadata they need in order to make a showing of "good cause."

One solution is for the Court to maintain a lenient standard for "good cause," and allow relevant facts to emerge early in the case to save time and money for litigants.

C. The Model Order Only Allows Email Production to Occur After the Parties Have Exchanged Initial Disclosures of Basic Documents and Information on the Critical Systems Storing the Email

The Model Order attempts to force the parties to hold off on email production until after initial disclosures regarding the patents, the prior art, and relevant financial information.[18]

---

[16] E-Discovery Model Order, *supra* note 2, at ¶ 5.

[17] *See* DISPUTE RESOLUTION AND E-DISCOVERY (Daniel B. Garrie & Yoav M. Griver eds., 2012).

[18] E-Discovery Model Order, *supra* note 2, at ¶ 8.

However, to encourage focused and reasonable email production, it is respectfully suggested that the Model Order also should require the parties to define their respective technology systems involved with email. This information is critical to allowing the parties to draft email requests that are reasonable and narrowly tailored, as required by the Model Order.[19]

For example, a party might craft a request for email that is narrowly tailored and appears reasonable,[20] but that request still could be unreasonable if the party seeks email that is five years old and is only stored on disk backup in Germany. In this example, the cost of production given the medium and location makes an apparently narrow and reasonable request unreasonable in practice, and may require an even more refined request. The parties should be required to identify and disclose their respective technology systems involved with email, so that such issues may be identified before email requests are issued. One possible solution is for the Model Order to be amended to require the parties to exchange information about their IT systems at the earliest stage of the litigation, enabling both sides to effectively organize their forthcoming search requests.

---

[19] E-Discovery Model Order, *supra* note 2, at ¶ 6 ("To obtain email parties must propound specific email production requests") and ¶ 7 ("Email production requests shall only be propounded for specific issues, rather than general discovery of a product or business").

[20] *See, e.g.*, McGrath v. United States, 103 Fed. Cl. 658 (Fed. Cl. 2012). In *McGrath*, the United States Court of Federal Claims considered a proposed discovery order that contained some of, but not all, the provisions from the Model Order. Among other things, the parties were eventually ordered to cooperate to identify the proper custodians, proper search terms, and proper timeframe before producing email, and "encouraged" to use narrowing search criteria (e.g., "and," "but not," "w/x") to limit email production.

D. The Model Order Should Consider Requiring the Parties to Perform Email Sampling Before Limiting the Number of Search Terms and Custodians to Five People and Terms

The Model Order presumptively limits the number of custodians and search terms for all email production requests to five terms and custodians per producing party for all such requests.[21] The intent is to control the exorbitant costs of production by minimizing what parties can request.[22] While well intentioned, this presumptive limit presents a challenging paradigm, because it is impossible for parties to be 100% accurate on terms and custodians – especially when they do not control the data. Consequently, it is our belief that, prior to the Court or parties selecting terms or custodians, they should apply common-sense:

1. Both parties should group search terms into high, medium, low value.
2. The parties should then take each group of search terms and identify applicable time frames and custodians. For example:

   High Group
   Dates: 02/2010 to 05/2011; 03/2005 to 04/2006
   Custodians: D. Smith; M. Jane
   Terms: Apple, Democrat, Republican, Libertarian
3. The opposing party should then sample each of the custodians using the search terms and dates for the group.
4. Re-order the terms and custodians.

Of course, the Court should mandate the application of the Model Order's strict number requirements, should the parties fail to mutually agree on a protocol, or if the terms the parties propose are inappropriate or indiscriminate in nature. In such circumstances, paragraph 11 of the Model Order provides for cost-shifting to the requesting party.

[21] E-Discovery Model Order, *supra* note 2, at ¶¶ 10, 11.

[22] *Id.* at 2, ¶¶ 6, 7.

IV. CONCLUSION

Courts and counsel should utilize the Model Order as a starting point for dialogue around e-discovery in patent disputes, but should also take into account the potential pitfalls that the Model Order presents. As the few cases have shown since the implementation of the Model Order, the court is willing, within reason, to allow parties to produce their own mutually agreeable protocol.[23] However, it remains to be seen what will happen in a case with unwilling parties whose case demands more than what the Model Order allows.

[23] *See, e.g.*, *McGrath*, 103 Fed. Cl. at 658 (modifying a proposed discovery order submitted by the parties that was based, in part, upon the Model Order).