SYRACUSE SCIENCE & TECHNOLOGY LAW REPORTER

VOLUME 22 SPRING 2010

TABLE OF CONTENTS

SYRACUSE SCIENCE & TECHNOLOGY LAW REPORTER

VOLUME 22 SPRING 2010

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 1, PAGE 1

"I, Robot – I, Criminal"—When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offenses

Gabriel Hallevy*

I. INTRODUCTION

Can society impose criminal liability upon robots? The technological world has changed rapidly. Simple human activities are being replaced by robots. As long as humanity used robots as mere tools, there was no real difference between robots and screwdrivers, cars or telephones. When robots became sophisticated, we used to say that robots "think" for us. The problem began when robots evolved from "thinking" machines into thinking machines (without quotation marks)—or Artificial Intelligence Robots (AI Robots). Could they become dangerous?

Unfortunately, they already are. In 1950, Isaac Asimov set down three fundamental laws of robotics in his science fiction masterpiece "I, Robot": (1) a robot may not injure a human being or, through inaction, allow a human being to come to harm; (2) a robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law; and (3) a robot must protect its own existence, as long as such protection does not conflict with the First or Second Laws.[1] These three fundamental laws are obviously contradictory.[2] What if a man orders a robot to hurt another person for the own good of the other person? What if the

* Associate Professor, Faculty of Law, Ono Academic College.

[1] ISSAC ASIMOV, I, ROBOT (1950).

[2] Isaac Asimov wrote in his introduction to THE REST OF ROBOTS (1964) that "[t]here was just enough ambiguity in the Three Laws to provide the conflicts and uncertainties required for new stories, and, to my great relief, it seemed always to be possible to think up a new angle out of the 61 words of the Three Laws."

robot is in police service and the commander of the mission orders it to arrest a suspect and the suspect resists arrest? Or what if the robot is in medical service and is ordered to perform a surgical procedure on a patient, the patient objects, but the medical doctor insists that the procedure is for the patient's own good, and repeats the order to the robot?

The main question in that context is which kind of laws or ethics are correct and who is to decide. In order to cope with these same problems as they relate to humans, society devised criminal law. Criminal law embodies the most powerful legal social control in modern civilization. People's fear of AI robots, in most cases, is based on the fact that AI robots are not considered to be subject to the law, specifically to criminal law. In the past, people were similarly fearful of corporations and their power to commit a spectrum of crimes, but since corporations are legal entities subject to criminal and corporate law, that kind of fear has been reduced significantly.[3]

The apprehension that AI robots evoke may have arisen due to Hollywood's depiction of AI robots in numerous films, such as "2001: A Space Odyssey,"[4] and the modern trilogy "The Matrix,"[5] in which AI robots are not subject to the law. However, it should be noted that Hollywood did treat AI robots in an empathic way by depicting them as human, as almost

---

[3] *See generally* John C. Coffee, Jr., *"No Soul to Damn: No Body to Kick": An Unscandalised Inquiry Into the Problem of Corporate Punishment*, 79 MICH. L. REV. 386 (1981); STEVEN BOX, POWER, CRIME AND MYSTIFICATION 16-79 (1983); Brent Fisse & John Braithwaite, *The Allocation of Responsibility for Corporate Crime: Individualism, Collectivism and Accountability*, 11 SYDNEY L. REV. 468 (1988).

[4] STANLEY KUBRICK, 2001: A SPACE ODYSSEY (1968).

[5] JOEL SILVER, THE MATRIX (1999); JOEL SILVER, LAURENCE WACHOWSKI AND ANDREW PAUL WACHOWSKI, THE MATRIX RELOADED (2003); JOEL SILVER, LAURENCE WACHOWSKI AND ANDREW PAUL WACHOWSKI, THE MATRIX REVOLUTIONS (2003).

human, or as wishing to be human.[6] This kind of treatment included, of course, clear subordination to human legal social control and to criminal law.

The modern question relating to AI robots becomes: Does the growing intelligence of AI robots subject them to legal social control, just as any other legal entity?[7] This article attempts to work out a legal solution to the problem of the criminal liability of AI robots. At the outset, a definition of an AI robot will be presented. Based on that definition, this article will then propose and introduce three models of AI robot criminal liability: (1) the perpetration-by-another liability model, (2) the natural-probable-consequence liability model, and (3) the direct liability model.

These three models might be applied separately, but in many situations, a coordinated combination of them (all or some of them) is required in order to complete the legal structure of criminal liability. Once we examine the possibility of legally imposing criminal liability on AI robots, then the question of punishment must be addressed. How can an AI robot serve a sentence of imprisonment? How can capital punishment be imposed on an AI robot? How can probation, a pecuniary fine, or the like be imposed on an AI robot? Consequently, it is necessary to formulate viable forms of punishment in order to impose criminal liability practically on AI robots.

---

[6] *See*, *e.g.*, STEVEN SPIELBERG, STANLEY KUBRICK, JAN HARLAN, KATHLEEN KENNEDY, WALTER F. PARKES AND BONNIE CURTIS, A.I. ARTIFICIAL INTELLIGENCE (2001).

[7] *See* in general, but not in relation to criminal law, *e.g.*, Thorne L. McCarty, *Reflections on Taxman: An Experiment in Artificial Intelligence and Legal Reasoning*, 90 HARV. L. REV. 837 (1977); Donald E. Elliott, *Holmes and Evolution: Legal Process as Artificial Intelligence*, 13 J. LEGAL STUD. 113 (1984); Thomas E. Headrick & Bruce G. Buchanan, *Some Speculation about Artificial Intelligence and Legal Reasoning*, 23 STAN. L. REV. 40 (1971); Antonio A. Martino, *Artificial Intelligence and Law*, 2 INT'L J.L. & INFO. TECH. 154 (1994); Edwina L. Rissland, *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, 99 YALE L.J. 1957 (1990).

II. WHAT IS AN AI ROBOT?

For some years, there has been significant controversy about the very essence of AI robots.[8] Futurologists have proclaimed the birth of a new species, *machina sapiens*, which will share the human place as intelligent creatures on Earth.[9] Critics have argued that a "thinking machine" is an oxymoron.[10] Machines, including robots, with their foundations of cold logic, can never be insightful or creative as humans are.[11] This controversy raises the basic questions of the essence of humanity (*i.e.*, do human beings function as thinking machines?) and of AI (*i.e.*, can there be thinking machines?).[12]

There are five attributes that one would expect an intelligent entity to have:[13] **(i) communication** (One can communicate with an intelligent entity. The easier it is to communicate with an entity, the more intelligent the entity seems. One can communicate with a dog, but not about Einstein's theory of relativity. One can communicate with a little child about Einstein's theory, but it requires a discussion in terms that a child can comprehend.); **(ii) mental knowledge** (An intelligent entity is expected to have some knowledge about itself.); **(iii)**

---

[8] Terry Winograd, *Thinking Machines: Can There Be? Are We?*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 167 (Derek Partridge & Yorick Wilks eds., 2006).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] For the formal foundations of AI, *see generally* Teodor C. Przymusinski, *Non-Monotonic Reasoning versus Logic Programming: A New Perspective, in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 49 (Derek Partridge & Yorick Wilks eds., 2006); Richard W. Weyhrauch, *Prolegomena to a Theory of Mechanized formal Reasoning*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 72 (Derek Partridge & Yorick Wilks eds., 2006).

[13] Roger C. Schank, *What is AI, Anyway?*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 3 (Derek Partridge & Yorick Wilks eds., 2006).

external knowledge (An intelligent entity is expected to know about the outside world, to learn about it, and utilize that information.); **(iv) goal-driven behavior** (An intelligent entity is expected to take action in order to achieve its goals.); and **(v) creativity** (An intelligent entity is expected to have some degree of creativity. In this context, creativity means the ability to take alternate action when the initial action fails. A fly that tries to exit a room and bumps into a window pane, tries to do that over and over again. When an AI robot bumps into a window, it tries to exit using the door).

Most AI robots possess these five attributes by definition.[14] Some 21st Century types of AI robots possess even more attributes that enable them to act in far more sophisticated ways. In November 2009, during the Supercomputing Conference in Portland Oregon ("SC 09"), IBM scientists and others announced that they succeeded in creating a new algorithm named "Blue Matter," which possesses the thinking capabilities of a cat.[15] This algorithm collects information from many units with parallel and distributed connections.[16] The information is integrated and creates a full image of sensory information, perception, dynamic action and reaction, and cognition.[17] This platform simulates brain capabilities, and eventually, it is supposed to simulate

[14] Schank, *supra* note 13, at 4-6.

[15] Chris Capps, *"Thinking" Supercomputer Now Conscious as a Cat*, UNEXPLAINABLE.NET, Nov. 19, 2009, http://www.unexplainable.net/artman/publish/article_14423.shtml; *see also* Super Computing, http://sc09.supercomputing.org.

[16] *Id.*

[17] *Id.*

real thought processes.[18] The final application of this algorithm contains not only analog and digital circuits, metal or plastics, but also protein-based biologic surfaces.[19]

An AI robot has a wide variety of applications.[20] A robot can be designed to imitate the physical capabilities of a human being, and these capabilities can be improved.[21] For instances, a robot is capable of being physically faster and stronger than a human being.[22] The AI software installed in it also enables the robot to calculate many complicated calculations faster and simultaneously, or to "think" faster.[23] An AI robot is capable of learning and of gaining experience, and experience is a useful way of learning.[24] All these attributes create the essence of an AI robot. AI robots and AI software are used in a wide range of applications in industry, military services, medical services, science, and even in games.[25]

---

[18] Capps, *supra* note 15.

[19] *Id.*

[20] *See*, *e.g.*, Yorick Wilks, *One Small Head: Models and Theories*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 121 (Derek Partridge & Yorick Wilks eds., 2006); Alan Bundy & Stellan Ohlsson, *The Nature of AI Principles*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 135 (Derek Partridge & Yorick Wilks eds., 2006); Thomas W. Simon, *Artificial Methodology Meets Philosophy*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 155 (Derek Partridge & Yorick Wilks eds., 2006).

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *See*, *e.g.*, William B. Schwartz, Ramesh S. Patil & Peter Szolovits, *Artificial Intelligence in Medicine Where Do We Stand*, 27 JURIMETRICS J. 362 (1987); Richard E. Susskind, *Artificial Intelligence, Expert Systems and the Law*, 5 DENNING L.J. 105 (1990).

III. MODELS OF THE CRIMINAL LIABILITY OF AI ROBOTS

The fundamental question of criminal law is the question of criminal liability, *i.e.*, whether the specific entity (human or corporation) bears criminal liability for a specific offense committed at a specific point in time and space.[26] In order to impose criminal liability upon a person, two main elements must exist.[27] The first is the factual element, *i.e.*, criminal conduct (*actus reus*), while the other is the mental element, *i.e.*, knowledge or general intent in relation to the conduct element (*mens rea*).[28] If one of them is missing, no criminal liability can be imposed.[29] The *actus reus* requirement is expressed mainly by acts or omissions.[30] Sometimes, other factual elements are required in addition to conduct, such as the specific results of that conduct and the specific circumstances underlying the conduct.[31] The *mens rea* requirement has various levels of mental elements.[32] The highest level is expressed by knowledge, while

---

[26] *See generally* JEROME HALL, GENERAL PRINCIPLES OF CRIMINAL LAW 70-211 (2d ed. 2005) (1960).

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *See* Walter Harrison Hitchler, *The Physical Element of Crime*, 39 DICK. L. REV. 95 (1934); MICHAEL MOORE, ACT AND CRIME: THE PHILOSOPHY OF ACTION AND ITS IMPLICATIONS FOR CRIMINAL LAW 5 (1993) (Tony Honore & Joseph Raz, eds., Oxford University Press 1993).

[31] *See* JOHN WILLIAM SALMOND, ON JURISPRUDENCE 505 (Glanville Williams ed., 11th ed. 1957); GLANVILLE WILLIAMS, CRIMINAL LAW: THE GENERAL PART 18 (2d ed., Steven & Sons Ltd. 1961); OLIVER W. HOLMES, THE COMMON LAW 54 (Mark DeWolf Howe ed., Harvard University Press 1923) (1881); Walter Wheeler Cook, *Act, Intention, and Motive in Criminal Law*, 26 YALE L.J. 645 (1917).

[32] HALL, *supra* note 26, at 105-45, 325-59.

sometimes it is accompanied by a requirement of intent or specific intention.[33] Lower levels are expressed by negligence (a reasonable person should have known),[34] or by strict liability offenses.[35]

No other criteria or capabilities are required in order to impose criminal liability, not from humans, nor from any other kind of entity, including corporations and AI robots.[36] An entity might possess further capabilities; however, in order to impose criminal liability, the existence of *actus reus* and *mens rea* in the specific offense is quite enough.[37] As far as known to science, a spider is capable of acting, but it is incapable of formulating the *mens rea* requirement; therefore, a spider bite bears no criminal liability. A parrot is capable of repeating words it hears, but it is incapable of formulating the *mens rea* requirement for libel. In order to impose criminal liability on any kind of entity, it must be proven that the above two elements

[33] *See generally* J. Ll. J. Edwards, *The Criminal Degrees of Knowledge*, 17 MOD. L. REV. 294, 295 (1954); Rollin M. Perkins, *"Knowledge" as a Mens rea Requirement*, 29 HASTINGS L.J. 953 (1978); *and see*, *e.g.*, United States v. Youts, 229 F.3d 1312, 1316 (10th Cir. 2000); United States v. Spinney, 65 F.3d 231, 235 (1st Cir. 1995); People v. Steinberg, 595 N.E.2d 845, 847 (N.Y. 1992); State v. Sargent, 594 A.2d 401, 403 (Vt. 1991); State v. Wyatt, 482 S.E.2d 147, 150 (W. Va. 1996).

[34] *See*, *e.g.*, Jerome Hall, *Negligent Behaviour Should Be Excluded from Penal Liability*, 63 COLUM. L. REV. 632, 632 (1963); Robert P. Fine & Gary M. Cohen, *Is Criminal Negligence a Defensible Basis for Criminal Liability?*, 16 BUFF. L. REV. 749, 780 (1966).

[35] *See*, *e.g.*, Jeremy Horder, *Strict Liability, Statutory Construction and the Spirit of Liberty*, 118 L. Q. REV. 458, 458 (2002); Francis Bowes Sayre, *Public Welfare Offenses*, 33 COLUM. L. REV. 55, 55 (1933); Stuart P. Green, *Six Senses of Strict Liability: A Plea for Formalism*, *in* APPRAISING STRICT LIABILITY 1 (A. P. Simester ed., 2005); A. P. Simester, *Is Strict Liability Always Wrong?*, *in* APPRAISING STRICT LIABILITY 21 (A. P. Simester ed., 2005).

[36] HALL, *supra* note 26.

[37] *Id.* at 185-86.

existed.[38] Thus, when it has been proven that a person committed the criminal act knowingly or with criminal intent, that person is held criminally liable for that offense.[39] The relevant question concerning the criminal liability of AI robots is: How can these entities fulfill the two requirements of criminal liability? This article proposes the imposition of criminal liability on AI robots using three possible models of liability: *(A)* the Perpetration-by-Another liability model; *(B)* the Natural-Probable-Consequence liability model; and *(C)* the Direct liability model. The following is an explanation of these possible models:

A. The Perpetration-by-Another Liability Model: AI Robots as Innocent Agents

This first model does not consider the AI robot as possessing any human attributes. The AI robot is considered an innocent agent. Accordingly, due to that legal viewpoint, a machine is a machine, and is never human. However, one cannot ignore an AI robot's capabilities, as previously mentioned.[40] Pursuant to this model, these capabilities are insufficient to deem the AI robot a perpetrator of an offense. These capabilities resemble the parallel capabilities of a mentally limited person, such as a child, or of a person who is mentally incompetent or who lacks a criminal state of mind.[41] Legally, when an offense is committed by an innocent agent, like when a person causes a child,[42] a person who is mentally incompetent[43] or who lacks a

[38] HALL, *supra* note 26.

[39] *Id.* at 105-45, 183.

[40] *See* discussion *supra* Part II.

[41] HALL, *supra* note 26, at 232.

[42] *See*, *e.g.*, Maxey v. United States, 30 App. D.C. 63 (1907); Commonwealth v. Hill, 11 Mass. 136 (1814); R. v. Michael, 169 Eng. Rep. 48 (1840).

criminal state of mind to commit an offense,[44] that person is criminally liable as a perpetrator-by-another.[45] In such cases, the intermediary is regarded as a mere instrument, albeit a sophisticated instrument, while the party orchestrating the offense (the perpetrator-by-another) is the real perpetrator as a principal in the first degree and is held accountable for the conduct of the innocent agent.[46] The perpetrator's liability is determined on the basis of that conduct[47] and his own mental state.[48]

The derivative question relative to AI Robots is: Who is the perpetrator-by-another? There are two candidates: the first is the programmer of the AI software installed in the specific robot and the second is the user. A programmer of AI software might design a program in order to commit offenses via the AI robot. For example, a programmer designs software for an operating robot. The robot is intended to be placed in a factory, and its software is designed to torch the factory at night when no one is there. The robot committed the arson, but the programmer is deemed the perpetrator. The second person who might be considered the perpetrator-by-another is the user of the AI robot. The user did not program the software, but he

---

[43] *See*, *e.g.*, Johnson v. State, 38 So. 182 (Ala. 1904); People v. Monks, 24 P.2d 508 (Cal. Dist. Ct. App. 1933).

[44] *See*, *e.g.*, United States v. Bryan, 483 F.2d 88 (3rd Cir. 1973); Boushea v. United States, 173 F.2d 131 (8th Cir. 1949); People v. Mutchler, 140 N.E. 820 (Ill. 1923); State v. Runkles, 605 A.2d 111 (Md. 1992); Parnell v. State, 912 S.W.2d 422 (Ark. 1996); State v. Thomas, 619 S.W.2d 513 (Tenn. 1981).

[45] *See generally* Morrisey v. State, 620 A.2d 207 (Del. 1993); State v. Fuller, 552 S.E.2d 282 (S.C. 2001); Gallimore v. Commonwealth, 436 S.E.2d 421 (Va. 1993).

[46] *Id.*

[47] *See generally* Dusenbery v. Commonwealth, 263 S.E.2d 392, 392 (Va. 1980).

[48] *See generally* United States v. Tobon-Builes, 706 F.2d 1092 (11th Cir. 1983); United States v. Ruffin, 613 F.2d 408 (2nd Cir. 1979).

uses the AI robot, including its software, for his own benefit. For example, a user purchases a servant-robot, which is designed to execute any order given by its master. The specific user is identified by the robot as that master, and the master orders the robot to assault any invader of the house. The robot executes the order exactly as ordered. This is not different than a person who orders his dog to attack any trespasser. The robot committed the assault, but the user is deemed the perpetrator.

In both scenarios, the actual offense was committed by the AI robot. The programmer or the user did not perform any action conforming to the definition of a specific offense; therefore, they do not meet the *actus reus* requirement of the specific offense. The perpetration-by-another liability model considers the action committed by the AI robot as if it had been the programmer's or the user's action. The legal basis for that is the instrumental usage of the AI robot as an innocent agent. No mental attribute required for the imposition of criminal liability is attributed to the AI robot.[49] When programmers or users use an AI robot instrumentally, the commission of an offense by the AI robot is attributed to them. The mental element required in the specific offense already exists in their minds.[50] The programmer had criminal intent when he ordered the commission of the arson, and the user had criminal intent when he ordered the commission of the assault, even though these offenses were actually committed through an AI robot.

This liability model does not attribute any mental capability, or any human mental capability, to the AI robot. According to this model, there is no legal difference between an AI robot and a screwdriver or an animal. When a burglar uses a screwdriver in order to open up a

[49] The AI robot is used as an instrument and not as a participant, although it uses its features of processing information. *See* George R. Cross & Cary G. Debessonet, *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, 1 HIGH TECH. L.J. 329, 362 (1986).

[50] HALL, *supra* note 26.

window, he uses the screwdriver instrumentally, and the screwdriver is not criminally liable. The screwdriver's "action" is, in fact, the burglar's. This is the same legal situation when using an animal instrumentally. An assault committed by a dog by order of its master is, in fact, an assault committed by the master.

This kind of legal model might be suitable for two types of scenarios. The first scenario is using an AI robot to commit an offense without using its advanced capabilities. The second scenario is using a very old version of an AI robot, which lacks the modern advanced capabilities of the modern AI robots. In both scenarios, the use of the AI robot is instrumental; it is usage of an AI robot, given its ability to execute an order, to commit an offense. A screwdriver cannot execute such an order; a dog can. A dog cannot execute complicated orders; an AI robot can.[51]

The perpetration-by-another liability model is not suitable when an AI robot decides to commit an offense based on its own accumulated experience or knowledge. This model is not suitable when the software of the AI robot was not designed to commit the specific offense, but was committed by the AI robot nonetheless. This model is also not suitable when the specific AI robot functions not as an innocent agent, but as a semi-innocent agent.[52] However, the perpetration-by-another liability model might be suitable when a programmer or user makes instrumental usage of an AI robot, but without using the AI robot's advanced capabilities. The legal result of applying this model is that the programmer and the user are both criminally liable for the specific offense committed, while the AI robot has no criminal liability whatsoever.

---

[51] *Compare* Andrew J. Wu, *From Video Games to Artificial Intelligence: Assigning Copyright Ownership to Works Generated by Increasingly Sophisticated Computer Programs*, 25 AIPLA Q.J. 131 (1997), *with* Timothy L. Butler, *Can a Computer be an Author: Copyright Aspects of Artificial Intelligence*, 4 HASTINGS COMM. & ENT. L.J. 707 (1982).

[52] *See generally* NICOLA LACEY & CELIA WELLS, RECONSTRUCTING CRIMINAL LAW: CRITICAL PERSPECTIVES ON CRIME AND THE CRIMINAL PROCESS 53 (2d ed. 1998).

B. The Natural-Probable-Consequence Liability Model: Foreseeable Offenses Committed by AI Robots

The second model of criminal liability assumes deep involvement of the programmers or users in the AI robot's daily activities, but without any intention of committing any offense via the AI robot. For instance, one scenario would be when an AI robot commits an offense during the execution of its daily tasks. The programmers or users had no knowledge of the offense until it had already been committed. They did not plan to commit any offense, and they did not participate in any part of the commission of that specific offense.

An example of such a scenario is when an AI robot or software is designed to function as an automatic pilot. As part of the mission of flying the plane, the AI robot is programmed to protect the mission itself. During the flight, the human pilot activates the automatic pilot (which is the AI robot), and the program is initiated. At some point after activation of the automatic pilot, the human pilot sees an approaching storm and tries to abort the mission and return to base. The AI robot deems the human pilot's action as a threat to the mission and takes action in order to eliminate that threat; it may attempt to cut off the air supply to the pilot or activate the ejection seat. Whatever defense tactic is taken, the human pilot is killed as a result of the AI robot's actions. Obviously, the programmer had not intended to kill anyone, especially not the human pilot, but nonetheless, the human pilot was killed by the AI robot's programmed actions.

In this example, the first model is not legally suitable. The first model assumes *mens rea*, the criminal intent of the programmers or users to commit an offense via the instrumental use of some of the AI robot's capabilities.[53] This is not the legal situation in the case of the automatic pilot. In this case, the programmers or users had no knowledge of the committed offense; they had not planned it, and had not intended to commit the offense using the AI robot. For such

[53] *See* discussion *supra* Part III.A.

circumstances, the natural-probable-consequence liability model may create a more suitable legal response. This model is based upon the ability of the programmers or users to foresee the potential commission of offenses.

According to the second model, a person might be held accountable for an offense, if that offense is a natural and probable consequence of that person's conduct. Originally, the natural-probable-consequence liability was used to impose criminal liability upon accomplices, when one committed an offense, which had not been planned by all of them and which was not part of a conspiracy.[54] The established rule prescribed by courts and commentators is that accomplice liability extends to acts of a perpetrator that were a "natural and probable consequence"[55] of a criminal scheme that the accomplice encouraged or aided.[56] The natural-probable-consequence liability has been widely accepted in accomplice liability statutes and recodifications.[57]

Natural-probable-consequence liability seems to be legally suitable for situations where an AI robot committed an offense, but the programmer or user had no knowledge of it, had not intended it and had not participated in it. The natural-probable-consequence liability model only requires the programmer or user to be in a mental state of negligence, not more. Programmers or users are not required to know about any forthcoming commission of an offense as a result of

---

[54] *See generally* United States v. Powell, 929 F.2d 724 (D.C. Cir. 1991).

[55] *Id.*

[56] *See generally* WILLIAM M. CLARK & WILLIAM L. MARSHALL, LAW OF CRIMES 529 (7th ed. 1967); Francis Bowes Sayre, *Criminal Responsibility for the Acts of Another*, 43 HARV. L. REV. 689 (1930); *and see*, *e.g.*, People v. Prettyman, 926 P.2d 1013 (Cal. 1996); Chance v. State, 685 A.2d 351 (Del. 1996); Ingram v. United States, 592 A.2d 992 (D.C. 1991); Richardson v. State, 697 N.E.2d 462 (Ind. 1998); Mitchell v. State, 971 P.2d 813 (Nev. 1998); State v. Carrasco, 928 P.2d 939 (N.M. 1996); State v. Jackson, 976 P.2d 1229 (Wash. 1999).

[57] *See*, *e.g.*, United States v. Andrews, 75 F.3d 552, 553-57 (9th Cir. 1996); State v. Kaiser, 918 P.2d 629, 632-39 (Kan. 1996).

their activity, but are required to know that such an offense is a natural, probable consequence of their actions.

A negligent person, in a criminal context, is a person who has no knowledge of the offense; rather, a reasonable person should have known about it since the specific offense is a natural probable consequence of that person's conduct.[58] Thus, the programmers or users of an AI robot, who should have known about the probability of the forthcoming commission of the specific offense, are criminally liable for the specific offense, even though they did not actually know about it. This is the fundamental legal basis for criminal liability in negligence cases.[59] Negligence is, in fact, an omission of awareness or knowledge.[60] The negligent person omitted knowledge, not acts.[61]

The natural-probable-consequence liability model would permit liability to be predicated upon negligence, even when the specific offense requires a different state of mind.[62] This is not valid in relation to the person who personally committed the offense, but rather, is considered valid in relation to the person who was not the actual perpetrator of the offense, but was one of its intellectual perpetrators.[63] Reasonable programmers or users should have foreseen the

---

[58] *See generally* Robert P. Fine & Gary M. Cohen, *Is Criminal Negligence a Defensible Basis for Criminal Liability?*, 16 BUFF. L. REV. 749, 749-52 (1966); Herbert L.A. Hart, *Negligence, Mens rea and Criminal Responsibility*, *in* OXFORD ESSAYS IN JURISPRUDENCE 29 (1961); Donald Stuart, *Mens rea*, *in* NEGLIGENCE AND ATTEMPTS, 1968 CRIM. L. REV. 647 (1968).

[59] HALL, *supra* note 26, at 114-40.

[60] *Id.*

[61] *Id.*

[62] THE AMERICAN LAW INSTITUTE, MODEL PENAL CODE: OFFICIAL DRAFT AND EXPLANATORY NOTES § 2.05 (1962, 1985) [hereinafter Model Penal Code]; *and see*, *e.g.*, State v. Linscott, 520 A.2d 1067, 1069 (Me. 1987); People v. Luparello, 231 Cal. Rptr. 832 (Cal. Ct. App. 1987).

offense, and prevented it from being committed by the AI robot. However, the legal results of applying the natural-probable-consequence liability model to the programmer or user differ in two different types of factual cases. The first type of case is when the programmers or users were negligent while programming or using the AI robot but had no criminal intent to commit any offense. The second type of case is when the programmers or users programmed or used the AI robot knowingly and willfully in order to commit one offense via the AI robot, but the AI robot deviated from the plan and committed some other offense, in addition to or instead of the planned offense.

The first type of case is a pure case of negligence. The programmers or users acted or omitted negligently; therefore, there is no reason why they should not be held accountable for an offense of negligence, if there is such an offense in the specific legal system. Thus, as in the example above, where a programmer of an automatic pilot negligently programmed it to defend its mission with no restrictions on the taking of human life, the programmer is negligent and liable for the homicide of the human pilot. Consequently, if there is a specific offense of negligent homicide in that legal system, this is the most severe offense, for which the programmer might be held accountable because manslaughter or murder requires knowledge or intent.

The second type of case resembles the basic idea of the natural-probable-consequence liability in accomplice liability cases. The dangerousness of the very association or conspiracy whose aim is to commit an offense is the legal reason for more severe accountability to be imposed upon the cohorts. For example, a programmer programs an AI robot to commit a violent robbery of a bank, but the programmer did not program the AI robot to kill anyone.

---

[63] *See* sources cited *supra* note 62.

During the execution of the violent robbery, the AI robot kills one of the people present at the bank who resisted the robbery. In such cases, the criminal negligence liability alone is insufficient. The danger posed by such a situation far exceeds negligence.

As a result, according to the natural-probable-consequence liability model, when the programmers or users programmed or used the AI robot knowingly and willfully in order to commit one offense via the AI robot, but the AI robot deviated from the plan and committed another offense, in addition to or instead of the planned offense, the programmers or users shall be held accountable for the offense itself as if it had been committed knowingly and willfully. In the above example of the robbery, the programmer shall be held criminally accountable for the robbery (if committed), as well as for the killing as an offense of manslaughter or murder, which requires knowledge and intent.[64]

The question still remains: What is the criminal liability of the AI robot itself when the natural-probable-consequence liability model is applied? In fact, there are two possible outcomes. If the AI robot acted as an innocent agent, without knowing anything about the criminal prohibition, it is not held criminally accountable for the offense it committed. Under such circumstances, the actions of the AI robot were not different from the actions of the AI robot under the first model (the perpetration-by-another liability model[65]). However, if the AI robot did not act merely as an innocent agent, then the AI robot itself shall be held criminally liable for the specific offense directly, in addition to the criminal liability of the programmer or

---

[64] *See*, *e.g.*, United States v. Greer, 467 F.2d 1064 (7th Cir. 1972); People v. Cooper, 743 N.E.2d 32 (Ill. 2000); People v. Michalow, 128 N.E. 228 (N.Y. 1920); People v. Little, 107 P.2d 634 (Cal. Dist. Ct. App. 1941); People v. Cabaltero, 87 P.2d 364 (Cal. Dist. Ct. App. 1939); People v. Weiss, 9 N.Y.S.2d 1 (N.Y. App. 1939); R v. Cunningham, 3 W.L.R. 76 (1957); R v. Faulkner, 13 Cox C.C. 550 (1876).

[65] *See supra* Part III.A.

user pursuant to the natural-probable-consequence liability model. The direct liability model of AI robots is the third model, as described hereunder.

C. The Direct Liability Model: AI Robots as Direct Subjects of Criminal Liability

The third model does not assume any dependence of the AI robot on a specific programmer or user. The third model focuses on the AI robot itself.[66] As discussed above, criminal liability for a specific offense is mainly comprised of the factual element (*actus reus*) and the mental element (*mens rea*) of that offense.[67] Any person attributed with both elements of the specific offense is held criminally accountable for that specific offense.[68] No other criteria are required in order to impose criminal liability.[69] A person might possess further capabilities, but, in order to impose criminal liability, the existence of the factual element and the mental element required to impose liability for the specific offense is quite enough.[70] In order to impose criminal liability on any kind of entity, the existence of these elements in the specific entity must be proven.[71] When it has been proven that a person committed the offense in question with

---

[66] *See generally* Steven J. Frank, *Tort Adjudication and the Emergence of Artificial Intelligence Software*, 21 SUFFOLK U. L. REV. 623 (1987); Sam N. Lehman-Wilzig, *Frankenstein Unbound: Towards a Legal Definition of Artificial Intelligence*, 13 FUTURES 442 (1981); Maruerite E. Gerstner, *Liability Issues with Artificial Intelligence Software*, 33 SANTA CLARA L. REV. 239 (1993); Richard E. Susskind, *Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning*, 49 MOD. L. REV. 168 (1986).

[67] HALL, *supra* note 26.

[68] *Id.*

[69] *Id.*

[70] *Id.* at 185-86.

[71] *Id.* at 183.

knowledge or intent, that person is held criminally liable for that offense.[72] The relevant questions regarding the criminal liability of AI robots are: How can these robots fulfill the requirements of criminal liability? Do AI robots differ from humans in this context?

An AI algorithm might have many features and qualifications far exceeding those of an average human, but such features or qualifications are not required in order to impose criminal liability.[73] When a human or corporation fulfills the requirements of both the factual element and the mental element, criminal liability is imposed.[74] If an AI robot is capable of fulfilling the requirements of both the factual element and the mental element, and, in fact, it actually fulfills them, there is presumptively nothing to prevent criminal liability from being imposed on that AI robot.

Generally, the fulfillment of the factual element requirement of an offense is easily attributed to AI robots. As long as an AI robot controls a mechanical or other mechanism to move its moving parts, any act might be considered as performed by the AI robot. Thus, when an AI robot activates its electric or hydraulic arm and moves it, this might constitute an act. For example, in the specific offense of assault, such an electric or hydraulic movement of an AI robot that hits a person standing nearby is considered as fulfilling the *actus reus* requirement of the offense of assault. When an offense might be committed due to an omission, it is even simpler. Under this scenario, the AI robot is not required to act at all; its very inaction is the legal basis for criminal liability, as long as there was a duty to act. If a duty to act is imposed upon the AI

[72] HALL, *supra* note 26, at 105-45, 183.

[73] *Id.* at 70-71; *see supra* Part II.

[74] *Id.*

robot and it fails to act, the *actus reus* requirement of the specific offense is fulfilled by way of an omission.

In most cases, the attribution of the mental element of offenses to AI robots is the real legal challenge. The attribution of the mental element differs from one AI technology to other. Most cognitive capabilities developed in modern AI technology are immaterial to the question of the imposition of criminal liability.[75] Creativity is a human feature that some animals have, but creativity is a not a requirement for imposing criminal liability.[76] Even the most uncreative persons are held criminally liable. The sole mental-state requirements to impose criminal liability are knowledge, intent, negligence, or the *mens rea* required in the specific offense and under the general theory of criminal law.[77]

Knowledge is defined as sensory reception of factual data and the understanding of that data.[78] Most AI systems are well equipped for such reception because they possess sensory receptors for sights, voices, physical contact, touch, and the like.[79] These receptors transfer the

---

[75] HALL, supra note 26.

[76] *Id.*

[77] *Id.*

[78] *See generally* WILLIAM JAMES, THE PRINCIPLES OF PSYCHOLOGY (1890); HERMANN VON HELMHOLTZ, THE FACTS OF PERCEPTION (1878). In this context, knowledge and awareness are identical. *See*, *e.g.*, United States v. Youts, 229 F.3d 1312 (10th Cir. 2000); United States v. Wert-Ruiz, 228 F.3d 250 (3th Cir. 2000); United States v. Ladish Malting Co., 135 F.3d 484 (7th Cir. 1998); United States v. Spinney, 65 F.3d 231 (1st Cir. 1995); United States v. Jewell, 532 F.2d 697 (9th Cir. 1976); State v. Sargent, 594 A.2d 401 (Vt. 1991); State v. Wyatt, 482 S.E.2d 147 (W. Va. 1996). *See also* Model Penal Code, *supra* note 62, at § 2.02(2)(b), which provides that, "A person acts *knowingly* with a respect to a material element of an offense when: (i) [if] he is *aware* that his conduct is of that nature or that such circumstances exist; and (ii) [if] he is *aware* that it is practically certain that his conduct will cause such a result" (emphasis added).

[79] *See generally* Margaret A. Boden, *Has AI Helped Psychology?*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 108 (Derek Partridge & Yorick Wilks eds., 2006); David Marr, *AI: A*

factual data received to central processing units that analyze the data.[80] The process of analysis in AI systems parallels that of human understanding.[81] The human brain understands and analyzes the data received by eyes, ears, and hands.[82] Advanced AI algorithms are trying to imitate human cognitive processes because these processes are not so different.[83]

Specific intent is the strongest of the mental element requirements.[84] Specific intent is the existence of a purpose or an aim that a factual event will occur.[85] The specific intent required to establish liability for murder is a purpose or an aim that a certain person will die.[86] As a result of the existence of such intent, the perpetrator of the offense commits the offense, *i.e.*, he performs the factual element of the specific offense.[87] This situation is not unique to humans,

---

Personal View, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 97 (Derek Partridge & Yorick Wilks eds., 2006).

[80] *See generally* Derek Partridge, *What's in an AI Program?*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 112 (Derek Partridge & Yorick Wilks eds., 2006).

[81] *Id.*

[82] *Id.*

[83] *See generally* Daniel C. Dennett, *Evolution, Error, and Intentionality*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 190 (Derek Partridge & Yorick Wilks eds., 2006); B. Chandraswkaran, *What Kind of Information Processing is Intelligence?*, *in* THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE 14 (Derek Partridge & Yorick Wilks eds., 2006).

[84] *See generally* Robert Batey, *Judicial Exploration of Mens rea Confusion at Common Law and Under the Model Penal Code*, 18 GA. ST. U. L. REV. 341 (2001).

[85] *See*, *e.g.*, Carter v. United States, 530 U.S. 255 (2000); United States v. Randolph, 93 F.3d 656 (9th Cir. 1996); United States v. Torres, 977 F.2d 321 (7th Cir. 1992); Frey v. United States, 708 So.2d 918 (Fla. 1998); State v. Neuzil, 589 N.W.2d 708 (Iowa 1999); State v. Daniels, 109 So.2d 896 (La. 1958); People v. Disimone, 650 N.W.2d 436 (Mich. Ct. App. 2002); People v. Henry, 607 N.W.2d 767 (Mich. Ct. App. 1999).

[86] For the intent-to-kill murder, *see* WAYNE R. LAFAVE, CRIMINAL LAW 733-34 (4th ed. 2003).

[87] *Id.*

and an AI robot might be programmed to have a similar purpose or an aim and to take actions to achieve that purpose. This is specific intent.[88]

One might assert that humans have feelings that cannot be imitated by AI robots, not even by the most advanced robots. Examples of such feelings are love, affection, hatred, or jealousy.[89] This theory might be correct in relation to the technology of the beginning of the 21st Century;[90] however, these feelings are rarely required in specific offenses. Most specific offenses are satisfied by knowledge of the existence of the factual element.[91] Few offenses require specific intent in addition to knowledge.[92] Almost all other offenses are satisfied by much less than that (*e.g.*, negligence, recklessness, strict liability). Perhaps in a few specific offenses that do require certain feelings (*e.g.*, crimes of racism, hate[93]), criminal liability cannot be imposed upon AI robots, which have no such feelings, but in any other specific offense, it is not a barrier.[94]

---

[88] LAFAVE, *supra* note 86.

[89] Capps, *supra* note 15.

[90] *Id.*

[91] HALL, *supra* note 26, at 632.

[92] *Id.*

[93] *See generally* Elizabeth A. Boyd, Richard A. Berk & Karl M. Hammer, *"Motivated by Hatred or Prejudice": Categorization of Hate-Motivated Crimes in Two Police Divisions*, 30 LAW & SOC'Y REV. 819, 842 (1996); Theresa Suozzi, F. Matt Jackson, Jeff Kauffman et al., *Crimes Motivated by Hatred: The Constitutionality and Impact of Hate Crimes Legislation in the United States*, 1 SYRACUSE J. LEGIS. & POL'Y 29 (1995).

[94] HALL, *supra* note 26, at 105-45.

If a person fulfills the requirements of both the factual element and the mental element of a specific offense, then the person is held criminally liable.[95] Why should an AI robot that fulfills all elements of an offense be exempt from criminal liability? One might argue that some segments of human society are exempt from criminal liability even if both the factual and mental elements have been established. Such segments of society are infants and the mentally ill.[96] A specific order in criminal law exempts infants from criminal liability.[97] The social rationale behind the infancy defense is to protect infants from the harmful consequences of the criminal process and to handle them in other social frameworks.[98] Do such frameworks exist for AI robots? The original legal rationale behind the infancy defense was the fact that infants are as

[95] HALL, *supra* note 26, at 70-211.

[96] *See supra* notes 40-45 and accompanying text.

[97] *Id.*; *and see*, *e.g.*, MINN. STAT. § 9913 (1927); MONT. REV. CODE § 10729 (1935); N.Y. PENAL CODE § 816 (1935); OKLA. STAT. § 152 (1937); UTAH REV. STAT. 103-i-40 (1933); State v. George, 54 A. 745 (Del. 1902); Heilman v. Commonwealth, 1 S.W. 731 (Ky. 1886); State v. Aaron, 4 N.J.L. 269 (N.J. 1818); McCormack v. State, 15 So. 438 (Ala. 1894); Little v. State, 554 S.W.2d 312 (Ark. 1977); Clay v. State, 196 So. 462 (Fla. 1940); *In re* Devon T., 584 A.2d 1287 (Md. 1991); State v. Dillon, 471 P.2d 553 (Idaho 1970); State v. Jackson, 142 S.W.2d 45 (Mo. 1940).

[98] *See generally* Frederick J. Ludwig, *Rationale of Responsibility for Young Offenders*, 29 NEB. L. REV. 521 (1950); *In re* Tyvonne, 558 A.2d 661 (Conn. 1989); Andrew Walkover, *The Infancy Defense in the New Juvenile Court*, 31 UCLA L. REV. 503 (1984); Keith Foren, *In Re Tyvonne M. Revisited: The Criminal Infancy Defense in Connecticut*, 18 Q. L. REV. 733 (1999); Michael Tonry, *Rethinking Unthinkable Punishment Policies in America*, 46 UCLA L. REV. 1751 (1999); Andrew Ashworth, *Sentencing Young Offenders*, *in* PRINCIPLED SENTENCING: READINGS ON THEORY AND POLICY 294 (Andrew von Hirsch, Andrew Ashworth & Julian Roberts eds., 3d ed. 2009); Franklin E. Zimring, *Rationales for Distinctive Penal Policies for Youth Offenders*, *in* PRINCIPLED SENTENCING: READINGS ON THEORY AND POLICY 316 (Andrew von Hirsch, Andrew Ashworth & Julian Roberts eds., 3d ed. 2009); Andrew von Hirsch, *Reduced Penalties for Juveniles: The Normative Dimension*, *in* PRINCIPLED SENTENCING: READINGS ON THEORY AND POLICY 323 (Andrew von Hirsch, Andrew Ashworth & Julian Roberts eds., 3d ed. 2009).

yet incapable of comprehending what was wrong in their conduct (*doli incapax*).[99] Later, children can be held criminally liable if the presumption of mental incapacity was refuted by proof that the child was able to distinguish between right and wrong.[100] Could that be similarly applied to AI robots? Most AI algorithms are capable of analyzing permitted and forbidden.

The mentally ill are presumed to lack the fault element of the specific offense, due to their mental illness (*doli incapax*).[101] The mentally ill are unable to distinguish between right and wrong (*cognitive capabilities*)[102] and to control impulsive behavior.[103] When an AI algorithm functions properly, there is no reason for it not to use all of its capabilities to analyze the factual data received through its receptors. However, an interesting legal question would be whether a defense of insanity might be raised in relation to a malfunctioning AI algorithm, when its analytical capabilities become corrupted as a result of that malfunction.

---

[99] SIR EDWARD COKE, INSTITUTIONS OF THE LAWS OF ENGLAND: THIRD PART 4 (6th ed. 2001) (1681).

[100] MATTHEW HALE, HISTORIA PLACITORUM CORONAE 23, 26 (1736) [MATTHEW HALE, HISTORY OF THE PLEAS OF THE CROWN (1736)]; *and see*, *e.g.*, McCormack v. State, 15 So. 438 (Ala. 1894); Little v. State, 554 S.W.2d 312 (Ark. 1977); *In re* Devon T., 584 A.2d 1287 (Md. 1991).

[101] Benjamin B. Sendor, *Crime as Communication: An Interpretive Theory of the Insanity Defense and the Mental Elements of Crime*, 74 GEO. L.J. 1371, 1380 (1986); Joseph H. Rodriguez, Laura M. LeWinn & Michael L. Perlin, *The Insanity Defense Under Siege: Legislative Assaults and Legal Rejoinders*, 14 RUTGERS L.J. 397, 406-07 (1983); Homer D. Crotty, *The History of Insanity as a Defence to Crime in English Common Law*, 12 CAL. L. REV. 105 (1924).

[102] *See generally* Edward de Grazia, *The Distinction of Being Mad*, 22 U. CHI. L. REV. 339 (1955); Warren P. Hill, *The Psychological Realism of Thurman Arnold*, 22 U. CHI. L. REV. 377 (1955); Manfred S. Guttmacher, *The Psychiatrist as an Expert Witness*, 22 U. CHI. L. REV. 325 (1955); Wilber G. Katz, *Law, Psychiatry, and Free Will*, 22 U. CHI. L. REV. 397 (1955); Jerome Hall, *Psychiatry and Criminal Responsibility*, 65 YALE L.J. 761 (1956).

[103] *See generally* John Barker Waite, *Irresistible Impulse and Criminal Liability*, 23 MICH. L. REV. 443, 454 (1925); Edward D. Hoedemaker, *"Irresistible Impulse" as a Defense in Criminal Law*, 23 WASH. L. REV. 1, 7 (1948).

When an AI robot establishes all elements of a specific offense, both factual and mental, it may be presumed that there is no reason to prevent imposition of criminal liability upon it for that offense. The criminal liability of an AI robot does not replace the criminal liability of the programmers or the users, if criminal liability is imposed on the programmers and users by any other legal path. Criminal liability is not to be divided, but rather, added. The criminal liability of the AI robot is imposed in addition to the criminal liability of the human programmer or user.

However, the criminal liability of an AI robot is not dependent upon the criminal liability of the programmer or user of that AI robot. As a result, if the specific AI robot was programmed or used by another AI robot, the criminal liability of the programmed or used AI robot is not influenced by that fact. The programmed or used AI robot shall be held criminally accountable for the specific offense pursuant to the direct liability model, unless it was an innocent agent. In addition, the programmer or user of the AI robot shall be held criminally accountable for that very offense pursuant to one of the three liability models, according to its specific role in the offense. The chain of criminal liability might continue, if more parties are involved, whether human or AI robots.

There is no reason to eliminate the criminal liability of an AI robot or of a human, which is based on complicity between them. An AI robot and a human might cooperate as joint perpetrators, as accessories and abettors, or the like; thus, the relevant criminal liability might be imposed on them accordingly. Since the factual and mental capabilities of an AI robot are sufficient to impose criminal liability—that is, if these capabilities satisfy the legal requirements of joint perpetrators, or of accessories and abettors—then the relevant criminal liability as joint perpetrators, accessories and abettors, or the like should be imposed irrespective of whether the offender is an AI robot or a human.

Not only positive factual and mental elements may be attributed to AI robots; rather, all relevant negative fault elements should be attributable to AI robots. Most of these elements are expressed by the general defenses in criminal law, *e.g.*, self-defense, necessity, duress, or intoxication. For some of these defenses (justifications),[104] there is no material difference between humans and AI robots since they relate to a specific situation (*in rem*), regardless of the identity of the offender. For example, an AI robot serving under the local police force is given an order to arrest a person illegally. If the order is not manifestly illegal, the executer of the order is not criminally liable.[105] In that case, there is no difference whether the executer is human or an AI robot.

For other defenses (excuses and exempts),[106] some applications should be adjusted. For example, the intoxication defense is applied when the offender is under the physical influence of an intoxicating substance (*e.g.*, alcohol or drugs). The influence of alcohol on an AI robot is minor, at most, but the influence of an electronic virus that is infecting the operating system of the AI robot might be considered parallel to the influence of intoxicating substances on humans.

---

[104] *See generally* JOHN C. SMITH, JUSTIFICATION AND EXCUSE IN THE CRIMINAL LAW (1989); Anthony M. Dillof, *Unraveling Unknowing Justification*, 77 NOTRE DAME L. REV. 1547 (2002); Kent Greenawalt, *Distinguishing Justifications from Excuses*, 49 LAW & CONTEMP. PROBS. 89 (1986); Kent Greenawalt, *The Perplexing Borders of Justification and Excuse*, 84 COLUM. L. REV. 949 (1984); Thomas Morawetz, *Reconstructing the Criminal Defenses: The Significance of Justification*, 77 J. CRIM. L. & CRIMINOLOGY 277 (1986); Paul H. Robinson, *A Theory of Justification: Societal Harm as a Prerequisite for Criminal Liability*, 23 UCLA L. REV. 266 (1975); Paul H. Robinson, *Testing Competing Theories of Justification*, 76 N.C. L. REV. 1095 (1998).

[105] *See generally* Michael A. Musmanno, *Are Subordinate Officials Penally Responsible for Obeying Superior Orders which Direct Commission of Crime?*, 67 DICK. L. REV. 221 (1963).

[106] *See generally* Peter Arenella, *Convicting the Morally Blameless: Reassessing the Relationship Between Legal and Moral Accountability*, 39 UCLA L. REV. 1511 (1992); Sanford H. Kadish, *Excusing Crime*, 75 CAL. L. REV. 257 (1987); Andrew E. Lelling, *A Psychological Critique of Character-Based Theories of Criminal Excuse*, 49 SYRACUSE L. REV. 35 (1998).

Some other factors might be considered as being parallel to insanity or loss of control. It may be concluded that the criminal liability of an AI robot, according to the direct liability model, is not different from the relevant criminal liability of a human. In some cases, some adjustments are necessary, but substantively, it is the very same criminal liability based upon the same elements and examined under the same light.

D. Hybrids: Coordinating the Models

The possible liability models described above are not alternative models.[107] These models might be applied in combination to create a full image of criminal liability in the specific context of AI robot involvement. None of the possible models is mutually exclusive. Thus, applying the second model is possible as a single model for the specific offense, and it is possible as one part of a combination of two of the legal models or of all three of them. When the AI robot plays the role of an innocent agent in the perpetration of a specific offense, and the programmer is the only person who directed that perpetration, the application of the perpetration-by-another model (the first liability model[108]) is the most appropriate legal model for that situation. In that same situation, when the programmer is itself an AI robot (when an AI robot programs another AI robot to commit a specific offense), the direct liability model (the third liability model[109]) is most appropriate to be applied to the criminal liability of the programmer of the AI robot. The third liability model in that situation is applied in addition to the first liability model, and not in lieu thereof. Thus, in such situations, the AI robot programmer shall be

[107] *See* discussion *supra* Parts III.A-C.

[108] *See* discussion *supra* Parts III.A.

[109] *See* discussion *supra* Parts III.C.

criminally liable, pursuant to a combination of the perpetration-by-another liability model and the direct liability model.[110]

If the AI robot plays the role of the physical perpetrator of the specific offense, but that very offense was not planned to be perpetrated, then the application of the natural-probable-consequence liability[111] model might be appropriate. The programmer might be deemed negligent if no offense had been deliberately planned to be perpetrated. Alternatively, the programmer might be held fully accountable for that specific offense if another offense had indeed been deliberately planned, but the specific offense that was perpetrated had not been part of the original criminal scheme. Nevertheless, when the programmer is not human, the direct liability model must be applied in addition to the simultaneous application of the natural-probable-consequence liability model; likewise, when the physical perpetrator is human while the planner is an AI robot.[112]

Hybrids of all three liability models create an opaque net of criminal liability. The combined and coordinated application of these three models reveals a new legal situation in the specific context of AI robots and criminal law. As a result, when AI robots and humans are involved, directly or indirectly, in the perpetration of a specific offense, it will be far more difficult to evade criminal liability. The social benefit to be derived from such a legal policy is of substantial value. All entities—human, legal or AI—become subject to criminal law. If the clearest purpose of the imposition of criminal liability is the application of legal social control in

[110] *See supra* Parts III.A and III.C.

[111] *See* discussion *supra* Parts III.B.

[112] *See supra* Parts III.B and III.C.

the specific society, then the coordinated application of all three models is necessary in the very context of AI robots.

IV. GENERAL PUNISHMENT ADJUSTMENT CONSIDERATIONS

Let us assume an AI robot is criminally liable. Let us assume it is indicted, tried and convicted. After the conviction, the court is supposed to sentence that AI robot. If the most appropriate punishment under the specific circumstances is one year of imprisonment, for example, how can an AI robot practically serve such a sentence? How can capital punishment, probation or even a fine be imposed on an AI robot? What is the practical meaning of imprisonment? Where no bank account is available for the sentenced AI robot, what is the practical significance of fining it?

Similar legal problems have been raised when the criminal liability of corporations was recognized.[113] Some asked how any of the legitimate penalties imposed upon humans could be applicable to corporations.[114] The answer was simple and legally applicable.[115] When a punishment can be imposed on a corporation as it is on humans, it is imposed without change.[116] When the court adjudicates a fine, the corporation pays the fine in the same way that a human

---

[113] *See generally* Gerard E. Lynch, *The Role of Criminal Law in Policing Corporate Misconduct*, 60 LAW & CONTEMP. PROBS. 23 (1997); Richard Gruner, *To Let the Punishment Fit the Organization: Sanctioning Corporate Offenders Through Corporate Probation*, 16 AM. J. CRIM. L. 1 (1988); Steven Walt & William S. Laufer, *Why Personhood Doesn't Matter: Corporate Criminal Liability and Sanctions*, 18 AM. J. CRIM. L. 263 (1991); John C. Coffee, Jr., *"No Soul to Damn: No Body to Kick": An Unscandalised Inquiry Into the Problem of Corporate Punishment*, 79 MICH. L. REV. 386 (1981); STEVEN BOX, POWER, CRIME AND MYSTIFICATION 16-79 (1983); Brent Fisse & John Braithwaite, *The Allocation of Responsibility for Corporate Crime: Individualism, Collectivism and Accountability*, 11 SYDNEY L. REV. 468 (1988).

[114] *Id.*

[115] *Id.*

[116] *Id.*

pays the fine and in the same way that a corporation pays its bills in a civil context.[117] However, when punishment of a corporation cannot be carried out in the same way as with humans, an adjustment is required.[118] Such is the legal situation vis-à-vis AI robots.

The punishment adjustment considerations examine the theoretical foundations of any applied punishment. These considerations are applied in a similar manner and are comprised of three stages. Each stage may be explained by a question: (1) What is the fundamental significance of the specific punishment for a human?; (2) How does that punishment affect AI robots?; and (3) What practical punishments may achieve the same significance when imposed on AI robots? The most significant advantage of these punishment adjustment considerations is that the significance of the specific punishment remains identical when imposed on humans and AI robots. This method of punishment adjustment considerations is referred to below in some of the punishments used in modern societies, *e.g.*, capital punishment, imprisonment, suspended sentencing, community service and fines.

Capital punishment is considered the most severe punishment for humans, and there is no consensus regarding its constitutionality among the various jurisdictions.[119] Capital punishment is the most effective method of incapacitating offenders as it relates to recidivism since, once the death sentence is carried out, the offender is obviously incapable of committing any further

---

[117] *See* sources cited *supra* note 113.

[118] *Id.*

[119] *See*, *e.g.*, GG art. 102 (for the abolition of capital penalty in Germany in 1949); Murder (Abolition of Death Penalty) Act, 1965, 13-14 Eliz. 2, c. 71 (for murder in Britain in 1965); *and* for the debate in the United States, *e.g.*, Wilkerson v. Utah, 99 U.S. 130 (1878); *In re* Kemmler, 136 U.S. 436 (1890); Gregg v. Georgia, 428 U.S. 153 (1979); Hunt v. Nuth, 57 F.3d 1327 (4th Cir. 1995); Campbell v. Wood, 18 F.3d 662 (9th Cir. 1994); Gray v. Lucas, 710 F.2d 1048 (5th Cir. 1983); People v. Daugherty, 256 P.2d 911 (Cal. 1953); Provenzano v. Moore, 744 So.2d 413 (Fla. 1999); Dutton v. State, 91 A. 417 (Md. 1914).

offense.[120] The significance of capital punishment for humans is the deprivation of life.[121] The "life" of an AI robot is its independent existence as an entity. Considering capital punishment's efficacy in incapacitating offenders, the practical action that may achieve the same results as capital punishment when imposed on an AI robot is deletion of the AI software controlling the AI robot. Once the deletion sentence is carried out, the offending AI robot is incapable of committing any further offenses. The deletion eradicates the independent existence of the AI robot and is tantamount to the death penalty.

Imprisonment is one of the most popular sentences imposed in western legal systems for serious crimes.[122] The significance of imprisonment for humans is the deprivation of human liberty and the imposition of severe limitations on human free behavior, freedom of movement and freedom to manage one's personal life.[123] The "liberty" or "freedom" of an AI robot

---

[120] *See generally* ROBERT M. BOHM, DEATHQUEST: AN INTRODUCTION TO THE THEORY AND PRACTICE OF CAPITAL PUNISHMENT IN THE UNITED STATES 74-78 (1999); Austin Sarat, *The Cultural Life of Capital Punishment: Responsibility and Representation in 'Dead Man Walking' and 'Last Dance'*, *in* THE KILLING STATE: CAPITAL PUNISHMENT IN LAW, POLITICS, AND CULTURE 226 (Austin Sarat ed., 1999); Peter Fitzpatrick, *"Always More to Do": Capital Punishment and the (De)Composition of Law*, *in* THE KILLING STATE: CAPITAL PUNISHMENT IN LAW, POLITICS, AND CULTURE 117 (Austin Sarat ed., 1999).

[121] *See generally* Franklin E. Zimring, *The Executioner's Dissonant Song: On Capital Punishment and American Legal Values*, *in* THE KILLING STATE: CAPITAL PUNISHMENT IN LAW, POLITICS, AND CULTURE 137 (Austin Sarat ed., 1999); Anthony G. Amsterdam, *Selling a Quick Fix for Boot Hill: The Myth of Justice Delayed in Death Cases*, *in* THE KILLING STATE: CAPITAL PUNISHMENT IN LAW, POLITICS, AND CULTURE 148 (Austin Sarat ed., 1999).

[122] *See generally* David J. Rothman, *For the Good of All: The Progressive Tradition in Prison Reform*, *in* HISTORY AND CRIME 271 (James A. Inciardi & Charles E. Faupel eds., 1980); MICHAEL WELCH, IRONIES OF IMPRISONMENT (2004); Roy D. King, *The Rise and Rise of Supermax: An American Solution in Search of a Problem?*, 1 PUNISHMENT & SOC'Y 163 (1999); CHASE RIVELAND, SUPERMAX PRISONS: OVERVIEW AND GENERAL CONSIDERATIONS (1999); JAMIE FELLNER & JOANNE MARINER, COLD STORAGE: SUPER-MAXIMUM SECURITY CONFINEMENT IN INDIANA (1997).

includes the freedom to act as an AI robot in the relevant area. For example, an AI robot in medical service has the freedom to participate in surgeries, or an AI robot in a factory has the freedom to manufacture. Considering the nature of a sentence of imprisonment, the practical action that may achieve the same effects as imprisonment when imposed on an AI robot is to put the AI robot out of use for a determinate period. During that period, no action relating to the AI robot's freedom is allowed, and thus its freedom or liberty is restricted.

Suspended sentencing is a very popular intermediate sanction in western legal systems for increasing the deterrent effect on offenders in lieu of actual imprisonment.[124] The significance of a suspended sentence for humans is the very threat of imprisonment if the human commits a specific offense or a type of specific offense.[125] If the human commits such an offense, a sentence of imprisonment will be imposed for the first offense in addition to the sentencing for the second offense.[126] As a result, humans are deterred from committing another offense and from becoming a recidivist offender.[127] Practically, a suspended sentence is imposed

---

[123] *See generally* Richard Korn, *The Effects of Confinement in the High Security Unit in Lexington*, 15 SOC. JUST. 8 (1988); Holly A. Miller, *Reexamining Psychological Distress in the Current Conditions of Segregation*, 1 J. CORRECTIONAL HEALTH CARE 39 (1994); FRIEDA BERNSTEIN, THE PERCEPTION OF CHARACTERISTICS OF TOTAL INSTITUTIONS AND THEIR EFFECT ON SOCIALIZATION (1979); BRUNO BETTELHEIM, THE INFORMED HEART: AUTONOMY IN A MASS AGE (1960); Marek M. Kaminski, *Games Prisoners Play: Allocation of Social Roles in a Total Institution*, 15 RATIONALITY & SOC'Y 188 (2003); JOHN IRWIN, PRISONS IN TURMOIL (1980); ANTHONY J. MANOCCHIO AND JIMMY DUNN, THE TIME GAME: TWO VIEWS OF A PRISON (1982).

[124] *See generally* MARC ANCEL, SUSPENDED SENTENCE (1971); Marc Ancel, *The System of Conditional Sentence or Sursis*, 80 L. Q. REV. 334 (1964).

[125] *Id.*

[126] *Id.*

[127] Anthony E. Bottoms, *The Suspended Sentence in England 1967-1978*, 21 BRITISH J. CRIMINOLOGY 1, 2-3 (1981).

only in the legal records.[128] No physical action is taken when a suspended sentence is imposed.[129] As a result, there is no difference between humans and AI robots. The statutory criminal records of the state do not differentiate between a suspended sentence imposed on humans, and those imposed on corporations or AI robots, as long as the relevant entity may be identified specifically and accurately.

Community service is also a very popular intermediate sanction in western legal systems in lieu of actual imprisonment.[130] In most legal systems, community service is a substitute for short sentences of actual imprisonment.[131] In some legal systems, community service is imposed coupled with probation so that the offender "pays a price" for the damages he caused by committing the specific offense.[132] The significance of community service for humans is compulsory contribution of labor to the community.[133] As discussed above, an AI robot can be engaged as a worker in very many areas.[134] When an AI robot works in a factory, its work is done for the benefit of the factory owners or for the benefit of the other workers in order to ease

---

[128] Bottoms, supra note 127.

[129] *Id.*

[130] *See generally* John Harding, *The Development of the Community Service*, *in* ALTERNATIVE STRATEGIES FOR COPING WITH CRIME 164 (Norman Tutt ed., 1978); HOME OFFICE, REVIEW OF CRIMINAL JUSTICE POLICY (1977); Andrew Willis, *Community Service as an Alternative to Imprisonment: A Cautionary View*, 24 PROBATION J. 120 (1977).

[131] *Id.*

[132] *See generally* Julie Leibrich, Burt Galaway & Yvonne Underhill, *Community Sentencing in New Zealand: A Survey of Users*, 50 FED. PROBATION 55 (1986); James Austin & Barry Krisberg, *The Unmet Promise of Alternatives*, 28 J. RES. IN CRIME & DELINQ. 374 (1982); Mark S. Umbreit, *Community Service Sentencing: Jail Alternatives or Added Sanction?*, 45 FED. PROBATION 3 (1981).

[133] *Id.*

[134] *See supra* p. 32.

and facilitate their professional tasks. In the same way that an AI robot works for the benefit of private individuals, it may work for the benefit of the community. When work for the benefit of the community is imposed on an AI robot as a compulsory contribution of labor to the community, it may be considered community service. Thus, the significance of community service is identical, whether imposed on humans or AI robots.

The adjudication of a fine is the most popular intermediate sanction in western legal systems in lieu of actual imprisonment.[135] The significance of paying a fine for humans is deprivation of some of their property, whether the property is money (a fine) or other property (forfeiture).[136] When a person fails to pay a fine, or has insufficient property to pay the fine, substitute penalties are imposed on the offender, particularly imprisonment.[137] The imposition of a fine on a corporation is identical to the imposition of a fine on a person, since both people and corporations have property and bank accounts. Thus, the payment of a fine is identical whether the paying entity is human or a corporate entity. However, most AI robots have no money or

---

[135] *See generally* GERHARDT GREBING, THE FINE IN COMPARATIVE LAW: A SURVEY OF 21 COUNTRIES (1982); NIGEL WALKER AND NICOLA PADFIELD, SENTENCING: THEORY, LAW AND PRACTICE (1996); Manfred Zuleeg, *Criminal Sanctions to be Imposed on Individuals as Enforcement Instruments in European Competition Law*, *in* EUROPEAN COMPETITION LAW ANNUAL 2001: EFFECTIVE PRIVATE ENFORCEMENT OF EC ANTITRUST LAW 451 (Claus-Dieter Ehlermann & Isabela Atanasiu eds., 2001); Judith A. Greene, *Structuring Criminal Fines: Making an 'Intermediate Penalty' More Useful and Equitable*, 13 JUST. SYS. J. 37 (1988); Manfred Zuleeg, *Criminal Sanctions to be Imposed on Individuals as Enforcement Instruments in European Competition Law*, *in* EUROPEAN COMPETITION LAW ANNUAL 2001: EFFECTIVE PRIVATE ENFORCEMENT OF EC ANTITRUST LAW 451 (Claus-Dieter Ehlermann & Isabela Atanasiu eds., 2001).

[136] *See generally* DOUGLAS C. MCDONALD, JUDITH A. GREENE & CHARLES WORZELLA, DAY-FINES IN AMERICAN COURTS: THE STATEN-ISLAND AND MILWAUKEE EXPERIMENTS (1992); STEVE UGLOW, CRIMINAL JUSTICE (1995).

[137] *See generally Use of Short Sentences of Imprisonment by the Court*, REPORT OF THE SCOTTISH ADVISORY COUNCIL ON THE TREATMENT OF OFFENDERS (1960); FIORI RINALDI, IMPRISONMENT FOR NON-PAYMENT OF FINES (1976).

property of their own, nor have they any bank accounts. In effect, the imposition of fines on AI robots may be problematic.

Assuming, however, if an AI robot did have its own property or money, the imposition of a fine on it would be identical to the imposition of a fine on humans or corporations. For most humans and corporations, property is gained through labor.[138] When paying a fine, such property resulting from labor is transferred to the state.[139] That labor might be transferred to the state in the form of property or directly as labor. As a result, a fine imposed on an AI robot might be collected as money or property and as labor for the benefit of the community. When the fine is collected in the form of labor for the benefit of the community, it is not different from community service as described above.[140]

Most common punishments are applicable to AI robots. The imposition of specific penalties on AI robots does not negate the nature of these penalties in comparison with their imposition on humans. Of course, some general punishment adjustment considerations are necessary in order to apply these penalties, but still, the nature of these penalties remains the same relative to humans and to AI robots.

V. CONCLUSION

If all of its specific requirements are met, criminal liability may be imposed upon any entity—human, corporate or AI robot. Modern times warrant modern legal measures in order to resolve today's legal problems. The rapid development of Artificial Intelligence technology requires current legal solutions in order to protect society from possible dangers inherent in

---

[138] JOHN LOCKE, TWO TREATISES OF GOVERNMENT (1689).

[139] *See supra* note 135.

[140] *See supra* pp. 33-34.

technologies not subject to the law, especially criminal law. Criminal law has a very important social function—that of preserving social order for the benefit and welfare of society. The threats upon that social order may be posed by humans, corporations or AI robots.

Traditionally, humans have been subject to criminal law, except when otherwise decided by international consensus. Thus, minors and mentally ill persons are not subject to criminal law in most legal systems around the world.[141] Although corporations in their modern form have existed since the 14th Century,[142] it took hundreds of years to subordinate corporations to the law, especially to criminal law.[143] For hundreds of years, the law stated that corporations are not subject to criminal law, as inspired by Roman law (*societas delinquere non potest*).[144] It was only in 1635 that an English court dared to impose criminal liability on a corporation.[145] Corporations participate fully in human life, and it was outrageous not to subject them to human laws since offenses are committed by corporations or through them. But, corporations have neither body nor soul. Legal solutions were developed so that in relation to criminal liability, they would be deemed capable of fulfilling all requirements of criminal liability, including

---

[141] *See* discussion *supra* Part III.A.

[142] WILLIAM SEARLE HOLDSWORTH, A HISTORY OF ENGLISH LAW 471-76 (1923).

[143] *Id.*

[144] *See generally* William Searle Holdsworth, *English Corporation Law in the 16th and 17th Centuries*, 31 YALE L.J. 382 (1922); WILLIAM ROBERT SCOTT, THE CONSTITUTION AND FINANCE OF ENGLISH, SCOTISH AND IRISH JOINT-STOCK COMPANIES TO 1720 462 (1912); BISHOP CARLETON HUNT, THE DEVELOPMENT OF THE BUSINESS CORPORATION IN ENGLAND 1800-1867 6 (Harvard University Press 1963).

[145] *See*, *e.g.*, Case of Langforth Bridge, 79 Eng. Rep. 919 (K.B. 1635); R v. Inhabitants of Clifton, 101 Eng. Rep. 280 (K.B. 1794); R v. Inhabitants of Great Broughton, 98 Eng. Rep. 418 (K.B. 1771); R v. Mayor of Stratford upon Avon, 104 Eng. Rep. 636 (K.B. 1811); R v. The Mayor of Liverpool, 102 Eng. Rep. 529 (K.B. 1802); R v. Saintiff, 87 Eng. Rep. 1002 (K.B. 1705).

factual and mental elements.[146] These solutions were embodied in models of criminal liability and general punishment adjustment considerations.[147] It worked. In fact, it is still working, and very successfully.[148]

Why should AI robots be different from corporations? AI robots are taking larger and larger parts in human activities, as do corporations. Offenses have already been committed by AI robots or through them. AI robots have no soul. Thus, there is no substantive legal difference between the idea of criminal liability imposed on corporations and on AI robots. It would be outrageous not to subordinate them to human laws, as corporations have been. As proposed by this article, models of criminal liability and general paths to impose punishment do exist. What else is needed?

---

[146] *See generally* Frederick Pollock, *Has the Common Law Received the Fiction Theory of Corporations?*, 27 L. Q. REV. 219 (1911).

[147] *Id.*

[148] *Id.*

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 2, PAGE 38

Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century

Stephen Hoffman*

INTRODUCTION

Imagine it is the year 2030. As you walk down your street to visit your favorite coffee shop, a camera mounted at the nearest intersection tracks your movements. Initially, you are just a set of pixels transmitted to a video screen somewhere; however, after your movement has been picked up by the camera, it uses algorithms based on general body and skull structure to pinpoint the location of your eyes. Once the camera has found your eyes, it projects an infrared beam of light into your eyes which would not be noticed because infrared light is not visible to the human eye. Using the reflection of the light from your retinas and choroids, the camera photographs the vasculature structure of your eyes and runs it against a database of known criminals, immigrants, and even people dissenting from popular opinion. If your retinal pattern matches that of a person listed in the database, the computer transmits this information to the proper authorities. All of this happens before you even step through the door of the coffee shop. This Orwellian[1] future of an omnipotent Big Brother is not consistent with a free democracy subservient to the people.

However, this is not the only worrisome issue presented by this scenario—what if private companies, instead of the government, are the ones running those cameras? What if a health

* J.D. Candidate 2010, University of Minnesota. The author would like to thank Professor Stephen Cribari for his help and suggestions on this work. Any substantive mistakes are my own.

[1] GEORGE ORWELL, 1984 (1949).

insurance company installs these cameras outside its offices to identify individuals and detect disorders and illnesses before they walk through the door? Retinal vascular patterns have been shown to anticipate future illnesses as well as conclusively identify several illnesses that the individual suffers from, and many of these are hereditary or genetic conditions. If the insurance company knows what you are susceptible to before you are personally aware, and uses this to refuse coverage or charge a higher premium for the policy you apply for, then it has appropriated something extremely private of yours without consent and may use this knowledge to profit from your supposed "condition," regardless of whether those future or current illnesses have manifested or will manifest themselves. Why should such an intrusive procedure be allowed without any concern for the privacy rights of those being examined?

I. BIOMETRICAL ANALYSIS AND ITS BACKGROUND

Retinal scanning, along with many other authentication techniques, falls under a branch of science known as biometrics. Biometrics or, more specifically, "biometric authentication" for purposes of this paper, is defined as the use of technology to automatically identify or verify the identity of people by physical or behavioral characteristics.[2] This idea of "automatic" identification is derived from the fact that, unlike most computer identification procedures such as entering a password or swiping a smart card, biometric identifiers use methods that require no additional knowledge but are still extremely difficult to counterfeit.[3] Some examples of biometric identifiers include fingerprints, facial structure, handwriting, and—which will be

[2] *See* JAMES WAYMAN ET AL., BIOMETRIC SYSTEMS 2 (2005); Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 MICH. TELECOMM. & TECH. L. REV. 541, 542 (2007).

[3] ROBERT HILL, RETINA IDENTIFICATION 1, *available at* http://www.cse.msu.edu/~cse891/Sect601/textbook/6.pdf.

discussed here—retinal structure.[4]

Biometric identification systems are grouped into two major categories: positive and negative identification.[5] Positive identification systems are used to test the hypothesis that the submitted image does belong to an individual enrolled in the system.[6] Positive identification systems are typically used in connection with high-security access or secure areas or networks. Such a system confirms that the individual is entitled to have access and is extremely useful in preventing multiple users from using a single enrolled identity. Negative identification systems, on the other hand, come into play when it is hypothesized that the submitted image does not belong to *any* individual in the system.[7] In essence, these systems are used to prevent a user from having multiple identities enrolled within the system.[8] This distinction between positive and negative identification systems is key in determining how the system will operate.

Biometric technologies fall into three general categories: high biometrics, lesser biometrics, or esoteric biometrics.[9] High biometrics are biometric technologies with a high accuracy rate and current working systems in operation, and also are based on "features that are

---

[4] Retinal scanning or imaging is actually somewhat of a misnomer. The scanning procedure uses infrared light to illuminate the retina, but the retina is "essentially transparent" to infrared light due to its wavelength. HILL, *supra* note 3, at 2. The reflection of the infrared light—which is used for the identification—is actually created by the collection of blood vessels in the choroid, which is just behind the retina. *Id.* at 2-3.

[5] WAYMAN, *supra* note 2, at 5.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 102 (1997).

considered truly consistent and unique."[10] These consist of fingerprint, retinal, and iris imaging.[11] Lesser biometrics, on the other hand, have reasonable accuracy and systems in operation but are not based on truly unique characteristics.[12] These characteristics include hand geometry, facial structure, and voice structure.[13] The term "esoteric biometrics" is used to describe experimental techniques or those in development.[14] Some examples of esoteric biometrics are vein measurement and the chemical composition of body odor.[15]

A. Theory and Advantages of Retinal Scanning

1. Introduction to Retinal Scanning Theory and the Scientific Method

Retinal scanning is widely accepted in the scientific community as being a valid method for authentication of people. This acceptance is based, as other reputable biometric systems are, on successful testing and hypothesizing using the scientific method.[16] Other systems and techniques which do not successfully utilize the scientific method yet are touted as accurate or true comprise a category known as "junk science."[17] Under the *Frye* standard,[18] which allowed

---

[10] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 102 (1997).

[11] *Id.* at 102-03.

[12] *Id.* at 105.

[13] *Id.* at 105-07.

[14] *Id.* at 108.

[15] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 108-09 (1997).

[16] CHRISTINE BECK LISSITZYN, FORENSIC EVIDENCE IN COURT 114-15 (2008).

[17] *See id.* at 113.

forensic evidence to be presented as long as the underlying theory was "generally accepted," false scientific theories and hypotheses such as the curative properties of bloodletting could be brought into court, usually in what is called the "battle of the experts."[19] However, the codification of Article VII of the Federal Rules of Evidence in 1975,[20] as well as the Supreme Court's determination that Article VII legislatively overruled *Frye*,[21] brought in a new standard for presenting scientific theories by experts. Under this new standard, delineated in *Daubert v. Merrell Dow Pharmaceuticals*,[22] expert testimony given regarding forensic science and biometrics is generally acceptable when it provides reliability and accuracy.[23] Because of this, a biometric measurement can almost exclusively be brought into court only if it possesses most or all of the five factors of an ideal biometric identifier.[24]

---

[18] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

[19] LISSITZYN, *supra* note 16, at 114. This "battle of the experts" still takes place today under the heightened standard announced in *Daubert*, but experts must present scientific evidence regarding the accuracy and reliability of the theory or method underlying the offered evidence. Daubert v. Merrell Dow Pharm., 509 U.S. 579, 589-91 (1993).

[20] FED. R. EVID. art. VII.

[21] *See generally Daubert*, 509 U.S. 579 (1993).

[22] *Id.*

[23] LISSITZYN, *supra* note 16, at 93. The *Frye* standard is still used by many courts and is even used as one prong of the *Daubert* test. *Id.*

[24] WAYMAN, *supra* note 2, at 3.

2. The Five Characteristics of the Ideal Biometric Identifier[25]

a. Distinctiveness

Retinal scanning, as mentioned above, is considered to be extremely accurate and based on the analysis of a truly unique, or distinctive, characteristic.[26] This biometric is determined by the blood vessel patterns in the human eye, which was first discovered to be unique in 1935.[27] A study performed in the 1950s examined similar characteristics between identical twins and found that, of all the factors compared, "retinal vascular patterns showed the least similarity."[28]

b. Robustness

However, uniqueness is not the sole criterion for whether a particular biometric analysis is useful for identification or authentication purposes—uniqueness is unimportant if the thing being measured is not consistent or stable, otherwise termed "robustness" in biometrics.[29] For example, fingerprints are very stable and consistent since they do not change over the course of one's life.[30] Retinal vascular patterns are similarly very stable and consistent and therefore make retinal imaging a strong biometrical method.[31]

---

[25] WAYMAN, *supra* note 2, at 3. The ideal biometric measure is distinct, robust, available, accessible, and accepted. *Id.*

[26] *See supra* notes 10-11 and accompanying text.

[27] HILL, *supra* note 3, at 2.

[28] *Id.*

[29] WAYMAN, *supra* note 2, at 542.

[30] Federal Bureau of Investigation, *Fingerprint Identification* 1, *available at* http://www.fbi.gov/hq/cjisd/ident.pdf.

[31] Robert Hill, the inventor of the first retinal identification system, posits that of all the physical features unique to individuals, "none is more stable than the retinal vascular pattern." HILL,

c. Availability

In an attempt to find the ideal biometric, availability is the next quality to be considered.[32] In order for a characteristic to be "available," the entire population or at least a substantial proportion of it should have the measure in multiples.[33] For example, fingerprints and retinal vascular patterns would be available characteristics.

d. Accessibility

An accessible measure is one that is "easy to image using electronic sensors."[34] Fingerprinting is a prime example of an accessible method because the person being measured must simply place his hand onto a screen, at which point electronic sensors can measure them.

e. Acceptability

The final, yet important, characteristic of an ideal biometric system is that people accept (rather than reject) the measurement being taken.[35] This generally requires two considerations. First, whether people find the measurement to not be so intrusive as to make them too uncomfortable during the assessment. To illustrate this clearly, imagine that people would be required to disrobe and have their genitalia measured as an identification technique (assuming that scientific studies had conclusively shown that human genitals are unique and consistent

---

supra note 3, at 2. However, as will be discussed shortly, retinal vasculature is not completely invulnerable to change over the person's lifetime and many medical and physical conditions can change the structure and appearance of a person's retinal vascular pattern.

[32] WAYMAN, *supra* note 2, at 541.

[33] *Id.* at 542.

[34] *Id.*

[35] *Id.* at 546.

among individuals). Due to the physical and emotional intrusiveness of the measurement and other things such as cultural or religious beliefs inconsistent with such a technique, this measurement would be very unlikely to be widely accepted by the public. Second, whether people accept the underlying theory on which the measurement is based. For example, fingerprinting has been generally accepted as being an extremely useful method of identification for the last 100 years and so has been accepted under this second element.

3. Two Primary Characteristics and Their Statistical Significance

The first two qualities described above, robustness and distinctiveness, also provide scientists and analysts with an objective standard by which to judge the efficacy of the system. The robustness of the system is measured by the "false non-match rate," or the probability that the image submitted will not match an enrolled image.[36] Statistically speaking, this is known as Type I error and is important in determining the accuracy of the system to a particular level of statistical significance.[37] The system's distinctiveness, on the other hand, is measured by its "false match rate," which is the probability that the image submitted will match another user's enrolled image.[38] In contrast, this probability is termed Type II error and is instrumental in determining the reliability of the method across the population.[39] With such normalizing of the system, the quality of the biometric measurement or system can be determined population-wide.

[36] WAYMAN, *supra* note 2, at 546.

[37] *Id.*

[38] *Id.*

[39] *Id.*

B. Uses for Biometric Systems

Biometric authentication systems generally have one of two uses: to verify an individual's identity or to identify a user based on his biometric credentials.[40] Verification, on one hand, is when a person known to the system and already identified has her identity confirmed by the biometric analysis. This is known as a "one-to-one" mapping since the individual is only compared with her own information to confirm her identity.[41] On the other hand, identification takes place when a person believed to be in the system uses biometric readings in order to match the individual in the entire database of those enrolled in the system.[42] Identification provides what is termed a "one-to-many" mapping because the individual is compared to others enrolled in the system as opposed to only her.[43]

One primary difficulty in making retinal imaging more widespread is user discomfort with the systems. Current systems require users to position their eyes, which must be wide-open for the duration of the scan, less than an inch from the retinal scanner while focusing on a

---

[40] Darcie Sherman, *Biometric Technology: The Impact on Privacy*, Law Research Institute Research Paper Series CLPE Research Paper No. 5/2005 3 (2005), *available at* http://ssrn.com/abstract=830049.

[41] Retinal scanning is considered a verification technique where the individual's retinal vascular pattern is compared to his alleged identity in the system. However, with advances in technology and dramatic increases in computer processing speeds, this may not be the case in the future. If Moore's Law is correct in its hypothesis of exponential increases in computer processor speeds over time, retinal images could be compared between an individual and other people enrolled in the system similar to the way fingerprints currently are.

[42] *See* source cited *supra* note 40, at 2-3.

[43] An example of identification is shown by fingerprint analysis and matching. The person's fingerprint is compared to those of a large number of persons enrolled in the system or even all of the persons enrolled. *Id.* at 2.

target.[44] The scan generally takes from 10-15 seconds and, if an accurate reading was not made such as due to blinking or eye movement, may need to be performed more than once.[45] Because of the obtrusiveness of the scan, retinal scanning and its counterpart iris scanning are slow to gain widespread public acceptance.

Another difficulty is that the retinal vascular patterns can give information besides simply identification or authentication, which is a major difference compared to other biometric methods. An examination of these patterns by an expert can indicate whether the individual suffers from common illnesses such as diabetes, arteriosclerosis, or hypertension, or from more unique circumstances such as AIDS, high blood pressure, or even intravenous drug abuse.[46] Because of this, retinal imaging and other biometric technologies cannot be used in all situations. To illustrate this, imagine that a health insurance company requires an individual to undergo a retinal scan both while creating his policy and at any emergency room he visits in order to ensure that he is the one using the health insurance and not some impostor. If the health insurance company can use these retinal images to determine which of an assortment of maladies a person suffers from, it could use this information—which is supposed to be used only for identification or authentication—to charge higher rates, provide more limited coverage, or even refuse coverage completely.

In addition, although the retinal vascular structure is very stable, it is not impervious to change. Age-related macular degeneration and other forms of degenerative retina disorders

---

[44] HILL, *supra* note 3, at 11-12.

[45] *Id.*

[46] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 115 (1997).

(including severe astigmatism) cause a large change in the pattern of the blood vessels used for biometrics.[47] Because of this, retinal scanning may not necessarily be reliable for verifying one's identity. This causes ideological problems in the context of the criminal justice system and convicted criminals. If a convicted criminal is released after having his retina scanned, he can "game" the system by simply bad genetics or improper eye care. If he is subsequently scanned again—say, on suspicion of committing another crime—his condition may allow him to avoid identification. Even if experts in retinal degeneration were called in to determine what, if any, medical conditions he could or did have through his retinal image, they could not view his later, altered retinal image and be able to deduce that it was the same man. Because of how complex and unpredictable the vascular patterns in the eye develop and the additional complexity and unpredictability of the alterations caused by retinal degeneration, it is impossible to know exactly how the vasculature will degenerate due to disease *X*. The human body is too variable on a population-wide scale and there are too many confounding factors that come into play to be able to predict exactly how the vascular pattern will change due to retinal degeneration.

Furthermore, expert review of retinal images can determine what medical conditions a person has and, if a genetic link is known or hypothesized to account for those conditions, indicate other conditions or disorders the person does or might suffer from.[48] Retinitis pigmentosa is an example of such a condition, with over 45 causative genes identified which

[47] For several illustrations from clinical studies of the different characteristics of ocular degeneration, *see* Eliot L. Berson, *Retinal Degenerations: Planning for the Future*, *in* RECENT ADVANCES IN RETINAL DEGENERATION 21-23 (Robert E. Anderson, Matthew M. LaVail & Joe G. Hollyfield eds., 2008).

[48] *Id.* at 23-24. "Over 100 genes have been implicated in human hereditary retinal degenerations." *Id.*

account for 50-60% of all cases.[49] As this suggests, if a retinal image suggests a person suffers from or is susceptible to this condition, there may be evidence that the individual suffers from or will suffer from other conditions which are caused by the same gene or genes. This is the case regardless of whether the person actually develops the feared conditions.

C. Retinal Scanning and Its Implications for the Right of Privacy

Although the uniqueness and consistence of retinal imaging and retinal vascular patterns support its use in identification and authentication, there are also equally plausible arguments against its use. For example, the fact that retinal vascular patterns are unique and consistent also shows one of its major flaws—compromise of a biometric system with this information would make it impossible to make that information secure. Unlike in traditional network security settings where users enter a password or swipe a smart card, such unique and personal information cannot be "reset" or changed to maintain the user's enrollment in the system. Therefore, a system based completely on retinal vascular patterns and no other biometric or alternative method of authentication or identification would be useless if an unauthorized person can access this information and help counterfeit the required credentials. Succinctly put, "[t]he theft of biometric information amounts to permanent identity theft."[50] Biometric analysis is useful if it measures an immutable and unique characteristic. However, if the characteristic being measured is truly immutable, the individual generally cannot and should not be required to

[49] *See* source cited *supra* note 47, at 23.

[50] Steven C. Bennett, *Privacy Implications of Biometrics*, 53 PRAC. LAW. 13, 17 (2007). Many scientists and biometric theorists strongly suggest using multimodal methods of biometric analysis. Therefore, rather than using only one biometric measure (e.g., retinal vascular pattern) as would be used in a unimodal system, multiple biometric measures would be taken to greatly reduce the opportunity or attractiveness of defrauding the system. *See generally* David Usher et al., *Ocular Biometrics: Simultaneous Capture and Analysis of the Retina and Iris*, *in* ADVANCES

alter or change his compromised characteristic in order to render his identity secure again.[51]

As discussed earlier in the health insurance hypothetical, another key issue is that of anonymity in biometrics. If such personal information as health conditions and illnesses, as well as statistical inferences regarding particular conditions (e.g., if African-Americans are more likely than members of any other ethnicity to suffer from diabetes, a random retinal scan of a diabetic individual may suggest that he is African-American) are illuminated by retinal scanning, then the scan is providing more information than simply that of verification or identification. However, the purpose of a biometric system is to verify or identify users of the system. If the system is used for more than that, it would not matter whether the individual is an enrolled user or an unaware party being subjected to the scan—the information could be collected from anyone and a centralized database or similar storage methods would be unnecessary. Because of this, the privacy implications of biometric analysis have to be considered in-depth.

Privacy, as Professor John D. Woodward, Jr. illustrates, generally falls under three categories: physical privacy, decisional privacy, and informational privacy.[52] Physical privacy is that which Justice Louis Brandeis described in his dissent in *Olmstead v. United States*—the "right to be let alone."[53] This is also known as the right to be free from contact by others or

---

IN BIOMETRICS 133 (Nalini K. Ratha & Venu Govindaraju eds., 2008).

[51] For example, if a person's fingerprint pattern is rendered unsecured because of unauthorized system access, the person, who has done nothing wrong or improper, should obviously not be forced to have his fingerprints chemically or surgically altered simply to maintain the integrity of the system.

[52] John D. Woodward, Jr., *The Law and the Use of Biometrics*, *in* HANDBOOK OF BIOMETRICS 357, 360-62 (Anil K. Jain et al. eds., 2008).

[53] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

monitoring agents.[54] The Founding Fathers valued this form of privacy highly and because of this drafted the Constitution with those concerns in mind, such as by ratifying the Fourth Amendment to the Constitution.

Decisional privacy, the next of the three categories, is focused on the freedom of letting individuals make private choices regarding personal matters without government interference.[55] An example of this type of privacy is shown in *Planned Parenthood of Southeastern Pennsylvania v. Casey*,[56] regarding procreation and contraception.

The third category with the most serious implications for biometric technologies, such as retinal scanning, is information privacy. Information privacy is the freedom of the person to limit access to certain personal information about him. This becomes a very serious issue when biometric measures give personal information without any concern for the person being analyzed. In addition, this raises many ethical problems when the information discovered is life-changing. For example, if a person is determined, after an analysis of her retinal vascular pattern, to have contracted AIDS, is the analyst or supervising firm required to disclose this information to the individual? Many would say yes, but what if a retinal image is only allowed if used in the course of verification or identification of a user? Since verification and identification are focused specifically on providing anonymity (hence, one major reason for having biometric analysis performed by a computer system), this would defeat any appearance of anonymity and thus be used in ways that biometrics are, or ought to be, by definition, unallowable.

---

[54] *See* source cited *supra* note 52, at 361.

[55] *Id.*

[56] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).

CONCLUSION

Biometric analysis is a very important and revolutionary method for identifying or verifying individuals. Although fingerprinting was the first generally accepted biometric that was tested, technology has come a long way in creating many other and more precise methods of analysis. Retinal scanning, otherwise known as retinal imaging or retinal vascular pattern analysis, is one of these recent technologies and provides many benefits over other biometric methods. However, there are several attendant issues that must also be considered. Particularly troubling are the privacy implications of retinal scanning when such a technique can be used to determine private information personal to the individual being scanned. Information such as current and prospective illnesses or conditions a person suffers from or will suffer from, as well as recognizing genetic links to other conditions, can be discovered simply by analyzing retinal vascular pattern. This must force a critical eye toward such a technique, which has its expressly given purpose to provide security while preserving anonymity.

In order to prevent an Orwellian future where "privacy" is merely a word found in the dictionary, there must be oversight to prevent Big Brother, or Big Business, from using this information to discriminate among members of the public. If we do not, the Thought Police shall no longer be restricted to fiction and freedom as we know it could be impaired beyond remedy.

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 3, PAGE 53

The Science of Identifying People by Their DNA, A Powerful Tool for Solving Crimes, Including Cold Cases From the Civil Rights Era

Ju-Hyun Yoo*

INTRODUCTION

Over fifty years ago, Emmett Till, a fourteen-year-old young black male, was found wrapped in barbed wire in a river in Mississippi.[1] No autopsy was ever conducted.[2] Two white men were arrested in 1955 for his murder, but were later acquitted because members of an all-white jury did not believe that the body found in the river was Emmett Till.[3] In 2004, the Federal Bureau of Investigation ("FBI") finally reopened its investigation into the murder.[4] One of the first steps taken by the FBI was to exhume the body and perform a DNA analysis by comparing the extracted DNA to the DNA profiles of Emmett Till's family members.[5] The

* J.D. candidate, Syracuse University College of Law, expected 2010. The author would like to thank Professor Janis L. McDonald for her support and helpful comments in advising this note.

[1] *Autopsy Done, Emmett Till Is Reburied*, N.Y. TIMES, Jun. 5, 2004, http://www.nytimes.com/2005/06/05/national/05till.html; *Murder case of Emmett Till no longer buried*, THE SEATTLE TIMES, May 5, 2005, http://seattletimes.nwsource.com/html/nationworld/2002263382_exhume05.html.

[2] *Id.*

[3] *People & Events: The Trial of J. W. Milam and Roy Bryant*, PUBLIC BROADCASTING SERVICE, http://www.pbs.org/wgbh/amex/till/peopleevents/e_trial.html.

[4] *See* sources cited *supra* note 1.

[5] *Id.*

analysis confirmed the body's identification as that of Emmett Till.[6] Although the two white men are now both dead, the DNA analysis and other evidence have indicated that there might have been other perpetrators who still remain alive.[7] The latest scientific tests, as shown in Emmett Till's case, have played a significant role in promoting justice by identifying leads to solve criminal cases.

In the United States, the collection and use of DNA, deoxyribonucleic acid, has greatly increased in criminal investigations over the last decade.[8] DNA forensics, the science of identifying people by their DNA, has become an indispensable criminal justice tool as it helps to identify criminals, victims' remains, and vindicate those who were wrongly convicted, including some awaiting execution.[9] Recent advancements in DNA technology, including the development of DNA database, have resulted in an increase of law enforcement's reliance on the use of DNA to solve all types of criminal cases, both old and recent.[10] Most importantly, DNA technology has become handy in making progress in the investigations of decades-old murder cases from the Civil Rights era, cases that everyone thought were closed.

The DNA databanks and the identifying profiles derived from them have had such a powerful and positive impact on the public by providing law enforcement authorities clues to solve crimes or make progress in their investigations, that there have been changes in laws such

---

[6] *See* sources cited *supra* note 1.

[7] *Id.*

[8] Dustin Hays, *The Science of DNA Forensics: Growing Pains and Ethical Challenges*, GENETICS & PUBLIC POLICY CENTER, May 4, 2007, http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=41.

[9] U.S. DEPARTMENT OF JUSTICE ADVANCING JUSTICE THROUGH DNA TECHNOLOGY (2008), http://www.justice.gov/ag/dnapolicybooktoc.htm.

[10] *Id.*

as legislation involving statutes of limitation.[11] These changes have benefitted cold cases, even those that are forty-year old.[12] Despite the positive contributions that the advancement of the DNA technology has been making to the general public, it has also raised significant questions involving ethical, social, and legal issues that mostly concern civil liberties.[13]

To better understand how the use of DNA and DNA databanks in criminal investigations have resulted in both positive and negative results, it is important to have a grasp of the history of the DNA technology, the development of DNA databases, which is discussed in the first part of this note. The discussion on the development of DNA technology covers the implementation of DNA databases both on Federal and state levels, with an emphasis on a recently developed DNA database in a Louisiana laboratory, which may likely be used as a model DNA database in other laboratories. Part II of this note examines the advantages of expanding DNA databases for criminal cases in general, with a focus on criminal cases from the Civil Rights era. Part II also discusses some of the issues raised by critics of expanding DNA databases.

[11] *See* Lauren O'Neil & Adam Fogarty, *The Impact of Daubert on Forensic Science*, 31 PEPP. L. REV. 323 (2004).

[12] *See* Beckwith v. Anderson, 89 F. Supp.2d 788 (Miss. 2000); *see also* Dustin Hays, *The Science of DNA Forensics: Growing Pains and Ethical Challenges*, GENETICS & PUBLIC POLICY CENTER, May 4, 2007, http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=41.

[13] *Id.*

DISCUSSION

I. BACKGROUND OF DNA DATABASES

1. Development of DNA Databases on Federal Level

The FBI has only recently begun using DNA testing for criminal investigations.[14] The FBI Laboratory Division created a DNA testing lab in 1988 and added DNA testing to criminal investigations.[15] As soon as State crime laboratories started using DNA testing technology, the Department of Justice decided to link these laboratories to the federal system and to each other.[16] The U.S. Department of Justice, through FBI, eventually developed the Combined DNA Index System, CODIS, "a fully integrated law enforcement database that allows [national, state, and local] crime laboratories throughout the United States to exchange DNA information about criminals, suspects, and victims of crime."[17]

Congress formally authorized CODIS for forensic analysis in 1994 by enacting the DNA Identification Act of 1994.[18] The Act authorized the FBI authority to establish a national DNA databank of (1) DNA identification records of persons convicted of crime, (2) analyses of DNA samples recovered from crime scenes, and (3) analyses of DNA samples recovered from

---

[14] Federal Bureau of Investigation, CODIS-NDIS Statistics, http://www.fbi.gov/hq/lab/codis/clickmap.htm.

[15] *Id.*; People v. Pizarro, 12 Cal. Rptr. 2d 436, 442 (Cal. Dist. Ct. App. 1992).

[16] *Id.*

[17] CODIS: Combined DNA Index System, *available at* http://www.enotes.com/forensic-science/codis-combined-dna-index-system.

[18] *See* 42 U.S.C § 14131 (1994).

unidentified human remains.[19] The Act also granted the FBI to set national standards for forensic DNA testing.[20] The established standard corresponds to "[thirteen] short DNA segments or short tandem repeats (STRs), which are regions of the genome that do not code for any traits but that, viewed in combination, provide a pattern unique to each individual."[21]

When the government first introduced DNA for law enforcement purposes, the collection and retention of DNA samples were limited to sexual offenders since these people were likely to leave behind biological evidence.[22] In October 1998, CODIS was launched on a national level.[23] Then in October 2004, President George W. Bush signed a law, the "Justice For All Act" (P.L. 108-405), which further expanded the CODIS system by allowing the states to collect DNA from all federal felons and insert the profiles into the system so that other states could view them.[24] Pursuant to Title II and III of the bill, new grant programs were made available to train criminal justice and medical personnel in the use of DNA evidence and promote the use of DNA technology to identify missing individuals.[25]

---

[19] STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS, OFFICE OF THE INSPECTOR GENERAL, AUDIT REPORT NO. 05-02 (2004), http://www.justice.gov/oig/reports/OJP/a0502/laws.htm.

[20] *Id.*

[21] *The FBI's Combined DNA Index System Program CODIS*, U.S. DEPARTMENT OF JUSTICE, (2000), *available at* http://www.dna.gov/rawmedia_repository/7d77e285_f2c0_4098_8863_fe744ce72e3b.

[22] *Id.*

[23] *Id.*

[24] *See* 18 U.S.C. § 3771 (2004).

[25] *Id.*

One year later, the government further enlarged the databanks by enacting another law, the DNA Fingerprinting Act of 2005, which authorized CODIS to include samples from any individual from whom collection was authorized under state law.[26] This Act of 2005 also authorized the collection of DNA from federal arrestees and from non-U.S. detainees to include them into the databases."[27] This legislation basically gave the Attorney General broad discretion in approving DNA testing authority to any federal agency and thus led to a gradual expansion of DNA data banks.[28]

As of February 2009, all fifty states along with Puerto Rico, the U.S. Army, and the FBI now participate in CODIS.[29] The National DNA Index (NDIS) has a list of over 6,297,765 offender profiles and 237,199 forensic profiles.[30] CODIS so far has assisted in more than 76,200 investigations.[31] These numbers indicate that laws have dramatically expanded forensic DNA databases, which have played a tremendous role in solving all kinds of cases, including cold cases from the Civil Rights era that were once believed to be unsolvable.

2. Development of DNA Databases on State Level

As previously mentioned, most states first began by inserting the DNA of sex offenders

---

[26] *See* DNA Fingerprint Act of 2005, Pub. No. L. 109-162, 119 Stat. 2960 (2005).

[27] *Id.*

[28] Tania Simoncelli & Sheldon Krimsky, *A New Era of DNA Collections: At What Cost to Civil Liberties?*, AMERICAN CONSTITUTION SOCIETY FOR LAW AND POLICY (2007), at 5, *available at* http://www.councilforresponsiblegenetics.org/pageDocuments/PG6T8WPI4A.pdf

[29] *Science and Technology in the Name of Justice, Part 2, FBI DNA Database Passes an Important Milestone*, FEDERAL BUREAU OF INVESTIGATION, Feb. 3, 2004, http://www.fbi.gov/page2/feb04/codis020304.htm

[30] *See* source cited *supra* note 14.

[31] *Id.*

into DNA databases so that they would increase protection of women and children from sexual attacks.[32] DNA submission of sex-offender records was not disputed since the general public viewed sexual assaults as unacceptable.[33] In 1994, a seven-year-old girl, Megan Kanka, was abducted, raped, and murdered by her neighbor, a convicted sex offender.[34] In response to Megan Kanka's shocking murder and the high number of repeat sex offenders, Congress along with all fifty states enacted laws requiring convicted sex offenders to submit DNA profiles.[35] This national agreement shows a movement towards the expansion of DNA databases.

Although a handful of states enacted DNA related laws before any federal legislation, a number of states had decided to expand DNA databases due to federal actions.[36] For instance, the DNA Fingerprinting Act provided to the states financial incentives to expand their DNA databanks.[37] Following the laws requiring the submission of DNA profiles from sex offenders, authorities also began demanding other individuals belonging to other categories of offenders to submit DNA profiles.[38] However, each state legislature independently determines whether DNA should be collected from arrestees or convicts.[39]

---

[32] Smith v. Doe, 538 U.S. 84, 89-90 (2003).

[33] D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413, 415 (2003).

[34] *Smith*, 538 U.S. at 89-90.

[35] *Id.*; *see also* Connecticut Dep't of Pub. Safety v. Doe, 538 U.S. 1, 4 (2003).

[36] *See* source cited *supra* note 26.

[37] *Id.*

[38] Kaye & Smith, *supra* note 33, at 416.

[39] *Id.*

In January 2007, twenty-five states introduced legislative proposals to expand DNA collections to some categories of arrestees.[40] This demonstrated that more states were moving towards the expansion of databanks, since only nine states in 2006 and eight states in 2005 introduced these same proposals.[41] These results demonstrate that federal actions, such as the increase in federal grants, have had an impact in the initiation of DNA databanks expansion.[42]

Despite the opposition of the enforcement of DNA testing of "other groups" from certain civil libertarian groups, all but four states, Idaho, Nebraska, New Hampshire, and Pennsylvania, require convicted felons to submit DNA into the federal database CODIS as of February 2009.[43] In addition, twenty-eight states collect DNA from juvenile offenders, nine collect DNA from those convicted of certain misdemeanors, and fifteen from arrestees.[44] The fifteen states are Alaska, Arizona, California, Kansas, Louisiana, Maryland, Michigan, Minnesota, New Mexico, North Dakota, South Carolina, South Dakota, Tennessee, Texas, and Virginia.[45]

Some states have even started retaining DNA samples from people belonging to "suspects" groups.[46] For instance, California passed California's Proposition 69, "the DNA

---

[40] Kaye & Smith, *supra* note 33, at 416; *see also* State v. Martin, 955 A.2d 1144, 1159 (Vt. 2008).

[41] *Id.*

[42] *Id.*; *see also* source cited *supra* note 26.

[43] *State Laws on DNA Data Banks Qualifying Offenses, Others Who Must Provide Sample*, National Conference of State Legislatures (Feb. 2009); *see also* Margot Sanger-Katz, *NH Rep: DNA Bill Needs Privacy Safeguard*, CONCORD MONITOR, Feb. 2. 2009, http://www.correctionsone.com/news/1783453-NH-Rep-DNA-bill-needs-privacy-safeguards.

[44] *Id.*

[45] *Id.*

[46] Simoncelli & Krimsky, *supra* note 28, at 7; DNA Fingerprint, Unsolved Crime and Innocence Protection Act, CAL. PENAL CODE § 295 (2004).

Fingerprint, Unsolved Crime and Innocence Protection Act", which has been authorizing the government since November 2004 to collect DNA samples and palm print impressions from suspects.[47] The purpose of this regulation was to retain the suspects' samples up to two years so that they can be compared when necessary and searched against the forensic identification profiles, including DNA profiles, stored in the files of the Department of Justice DNA data banks or databases.[48]

a. State of Louisiana

A number of Civil Rights-era murder cases took place in the State of Louisiana and many of them still remain unsolved. The development of DNA technology, such as the expansion of DNA databanks, can represent an essential tool to law enforcement in finally obtaining some answers to solve cold cases such as the murders that took place during the Civil Rights era. This may be one of the reasons why Louisiana was one of the first states to enact legislation and to start collecting DNA samples from arrestees for databasing purposes.[49]

In support of DNA database expansion, the state of Louisiana passed a law in 2006, House Bill 1140 Act 227, which designated Louisiana State University's Forensic Anthropology and Computer Enhancement Services (FACES) Laboratory as the "central repository for 'all unidentified human remains information and all missing person data collected' in Louisiana."'[50]

---

[47] *See also* sources cited *supra* note 46.

[48] *Id.* § III, art. 3(c)(2).

[49] LA. REV. STAT. § 15:609 (2004); *see generally* Louisiana State Police News Releases, http://www.lsp.org/lspnewsr.nsf/.

[50] Stanley Nelson, *Is Skull Found in Clayton Remains of JoeEd Edwards*, CONCORDIA SENTINEL, July 24, 2008, http://www.concordiasentinel.com/news.php?id=2163.

This legislation provides FACES Lab a significant yearly grant.[51] This grant allows the Lab to work towards their primary goal of compiling a comprehensive database of Louisiana's missing and unidentified human remains, including DNA, age, sex, race, ancestry, and all other identifying factors.[52]

For an effective compilation of information, the Lab works regularly with the Louisiana State Police Crime Lab, the North Louisiana Criminalistics Laboratory, coroners, and sheriff's offices, and uses an existing software package to gather all information on unidentified bodies and missing persons from state law enforcement by comparing data on unidentified remains to the data available on individuals who have been reported missing.[53]

The law passed in Louisiana in 2006 has given FACES Lab an opportunity to establish a DNA database that could be more complex than the existing CODIS.[54] As previously explained, CODIS is a database that contains DNA information about criminals, suspects, and victims of crimes inserted by crime laboratories throughout the United States.[55] However, the database operated by FACES Lab offers even more information than CODIS.[56] FACES Lab personnel have been given permission to collect available biological data and DNA samples from families

---

[51] Rob Anderson, *FACES Lab building Database of Missing Persons*, LSU TODAY, Nov. 5, 2004, http://www.lsu.edu/lsutoday/041105/.

[52] *Id.; see also* H.B. 1140 Act 227, Reg. Sess. (La. 2006), available at http://identifyla.lsu.edu/hb1140act227.pdf

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *See* sources cited *supra* notes 51-52.

of missing persons.[57] This means that FACES Lab may be able to create a more complex and effective Identification Data Analysis database than any other existing databases, because it will not only contain DNA information about criminals, suspects, victims of crimes, but also DNA information about certain families of victims.[58] This database will thus most likely increase successes in linking DNA in murder cases, including high-profile murder cases that were once believed to be unsolvable.

Due to this promising result in criminal investigations, even if Louisiana Law Enforcement and FACES Lab are currently compiling a database of missing and unidentified persons for the state of Louisiana only, there is a high possibility, as the director of FACES Lab predicts, that this unique identification data analysis project will soon become a model that can be used and shared with other agencies outside of Louisiana in the resolution of unidentified and missing persons case.[59] As a result, Louisiana may become the central location, where it will store and retrieve crucial information on hundreds of missing and unidentified persons on a local, regional, and state level.[60]

II. POSITIVE AND NEGATIVE RESULTS OF DNA DATABASE EXPANSION

1. Advantages of DNA Database Expansion

As previously stated, proponents of DNA database expansions argue that larger DNA databases help solve all types of crimes, including crimes from the Civil Rights era cold cases that were once believed to be unsolvable to more recently committed crimes, thereby stopping

---

[57] *See* sources cited *supra* notes 51-52.

[58] *Id.*

[59] *Id.*

[60] *Id.*

criminals before they can happen again.[61] For instance, the State of Virginia, which requires DNA profiles submission from all those arrested for violent felonies, claims to have solved hundreds of crimes by comparing profiles found in the arrestee database.[62] According to a study done in Chicago in 2005, at least "fifty-three murders and rapes could have been prevented if a DNA sample had been collected from all arrestees."[63] This study, an example among others, indicates that the expansion of DNA database helps to solve and prevent crimes.

a. Implications with the Statute of Limitation

The advantages that result from the expansion of DNA databases have led to changes in statutes of limitation for cases related to criminal charges. In a criminal case, a statute of limitations is a rule that establishes a time limit for prosecuting a crime based on the date when the offense occurred.[64] The purpose of a statute of limitations in a criminal case is to guarantee "the prompt prosecution of criminal charges and thereby to spare the accused of the burden of having to defend against stale charges after memories may have faded or evidence is lost."[65]

---

[61] *See* Human Genome Project Information, DNA Forensics (2009), http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml.

[62] *See* DNA TESTING FOR LAW ENFORCEMENT: LEGISLATIVE ISSUES FOR CONGRESS, CRS REPORT FOR CONGRESS (2006), *available at* http://www.house.gov/gallegly/issues/crime/crimedocs/RL32247.pdf.

[63] Eileen Sullivan, *Feds to Collect DNA From Every Person They Arrest*, THE HUFFINGTON POST, Apr. 16, 2008, http://www.huffingtonpost.com/2008/04/16/feds-to-collect-dna-from-_n_97100.html.

[64] *See* STATUTES OF LIMITATION IN FEDERAL CRIMINAL CASES: A SKETCH, CRS REPORT FOR CONGRESS RS 21221, ii (2007), *available at* http://www.fas.org/sgp/crs/misc/RL31253.pdf.

[65] *See id.*

A statute of limitations for federal crimes punishable by death does not exist.[66] States courts have also held that there is no statute of limitations for murder cases.[67] For instance in *Beckwith v. Anderson*, the court stated that "the Mississippi statute of limitations governing criminal charges does not impose a limitation period on the crime of murder."[68] In Louisiana, there is also no statute of limitation for murder cases.[69]

According to the President's DNA Initiative, advances in DNA technology and the creation of DNA databases are leading many criminal justice professionals to reevaluate time limits placed on the filing of criminal charges.[70] Many State legislatures have begun to extend the statutes of limitation because biological evidence can product reliable DNA analysis results even years after the commission of a crime.[71] Some states have eliminated the statutes of limitation for some crimes, in certain circumstances.[72]

These changes are essential for all crimes, but most certainly for cold cases from the Civil Rights era. As previously explained, the purpose of a statute of limitations in a criminal case is to guarantee "the prompt prosecution of criminal charges and thereby to spare the accused of the burden of having to defend against stale charges after memories may have faded or evidence

---

[66] *See* source cited *supra* note 64.

[67] Beckwith v. Anderson, 89 F. Supp.2d 788, 805 (Miss. 2000).

[68] *Id.*; MISS. CODE ANN. § 99-1-5 (2009).

[69] LA. CODE CRIM. PROC. ANN. art. 571 (2010).

[70] *See generally* Lauren O'Neil & Adam Fogarty, *The Impact of Daubert on Forensic Science*, 31 Pepp. L. Rev. 323 (2004); *see also Solving Cold Cases with DNA*, DNA INITIATIVE: ADVANCING CRIMINAL JUSTICE THROUGH DNA TECHNOLOGY, *available at* http://www.dna.gov/funding/cold_case/.

[71] *Id.*

[72] *Id.*

is lost."[73] However, despite this purpose, it would be beneficial for law enforcement to present new evidence found by using DNA technology in the interest of true justice. For instance, as we saw in Emmett Till's case, the FBI was able to exhume the body and retrieve a DNA sample to confirm that the body belonged to Emmett Till.[74] The statutes of limitation will likely be a critical issue if other perpetrators involved in the murder of Emmett Till were still alive today and later found by the FBI.[75]

b. <u>What could Louisiana Identification Data Analysis mean to the general public.</u>

Cold cases are usually among the most difficult and frustrating cases detectives face, especially if they involve racially motivated killings from the Civil Rights era. In order to identify deadly hate crimes that occurred before 1969 and that remained unsolved, many law enforcement agencies, prosecutors' offices, and crime labs across the nation have launched programs to review old cases.[76] These programs, often called "cold case units," have helped criminal justice officials to solve cases that have remained unsolved for years.[77] It was found that DNA evidence was "the linchpin" in solving most of these cases.[78]

For instance, in the 1963 murder case of Civil Rights activist Medgar Evers, DNA and other scientific evidence helped gain the 1994 conviction of White Supremacist Byron de La

---

[73] *See* source cited *supra* note 64, at 1.

[74] *See supra* note 1 and accompany text.

[75] *Id.*

[76] *Civil Rights: FBI Announces Partnership in Reviewing Cold Cases*, FEDERAL BUREAU OF INVESTIGATION, Feb. 27, 2007, *available at* http://www.fbi.gov/page2/feb07/coldcase022707.

[77] *Id.*

[78] *Id.*

Beckwith.[79] In 1991, the FBI exhumed Evers' body and removed bullet fragments, which were found to have come from the weapon used to kill Evers.[80]

Louisiana and several other states collect DNA profiles even from people arrested for misdemeanors, which has led and will hopefully lead to clues to solve all types of criminal cases, including those that occurred several decades ago.[81] For instance, LSU FACES lab is currently working to collect identification factors that could determine whether a human skull found in Clayton six years ago could be part of the remains of a black man who was reported missing in Concordia Parish, Louisiana, and presumed dead since July 12, 1964.[82] This case is one of many examples of a troubling unsolved murder case from the Civil Rights era.

FACES Lab forensic anthropologists are using the recently adopted Louisiana Identification Data Analysis to establish the identity of the discovered human skull.[83] Although this project will require time and effort, FACES Lab is hopeful because some family members of the man reported missing since 1964 still reside in Louisiana.[84] The family members may provide a sampling of DNA which could then be compared to the DNA extracted from the skull. This comparison may possibly lead to some clues and make progress in this unsolved case from the Civil Rights era.

---

[79] *See* Beckwith v. Anderson, 89 F. Supp.2d 788 (Miss. 2000).

[80] Charles Sheehan, *Body of Emmett Till Exhumed in Illinois*, CHI. TRIB., June 2, 2005, *available at* http://www.truthout.org/article/body-emmett-till-exhumed-in-illinois.

[81] *See* LA. REV. STAT. § 15:609 (2004).

[82] *See* source cited *supra* note 50.

[83] *Id.*

[84] *Id.*

If a database such as the Louisiana Identification Data Analysis were in place at an earlier time, crimes that are believed to have been committed by Ku Klux Klan members for racially motivated reasons may have been solved. Ku Klux Klan members are known to have committed numerous crimes in the South. It is also known that family members tend to join a Klan together. Thus, if other DNA databases, such as the one FACES Lab is currently developing, are created, there is a possibility for law enforcement to collect evidence that may result in positive outcomes.

Many crimes from the Civil Rights era still remain unsolved for numerous reasons. However, there may be something that we could do now. For example, we could maybe find some answers by expanding the newest technology, DNA databanks.

c. The Impact of Emmett Till Unsolved Civil Rights Crime Bill on Forensic Science

Following the passage of the DNA Identification Act of 1994 and the DNA Fingerprinting Act of 2005, "cold case units" have been able to gather biological evidence that may assist law enforcement authorities to solve crimes.[85] In addition to the legislation that permitted the expansion of DNA databanks, Congress in September 2008, enacted the Emmett Till Unsolved Civil Rights Crime Bill that would give the Justice Department more funding to investigate unsolved murders from the Civil Rights era.[86] The legislation was originally inspired from the case of Emmett Till.[87] The Bill provides $13.5 million annually over ten years to assist the FBI and other relevant agencies to pursue investigating cases, mostly in the South.[88]

---

[85] *See* source cited *supra* note 76.

[86] Emmett Till Unsolved Civil Rights Crime Act of 2007, Pub. L. No. 110-344, 122 Stat. 3934 (2008), *available at* http://www.govtrack.us/congress/billtext.xpd?bill=h110-923.

[87] *Id.*

[88] *Id.*

The federal funding for cold cases units had significantly decreased over the past years, but the enactment of the Emmett Till Bill will regenerate the funding for the investigation of cold cases, at least those that involve racially motivated killings.[89] Research shows that the federal grant funding for cold cases units totaled $14.2 million in 2005; however, the funding only reached $8.7 million in 2007.[90] For example, Louisiana was listed amongst the states receiving a fairly large sum of financial incentives from the federal government, but it only received from 2005 to 2008 a total of $1,026,395 for cold case units.[91] Due to a lack of funding, law enforcement has not been able to use forensic science services effectively within these past years.[92] Nevertheless, with the passage of the Emmett Till Bill, they may now increase the use of DNA databanks and possibly solve more criminal cases, at least some of those that occurred during the Civil Rights era.

d. Innocent Convicts

There are cases where innocent people have been incarcerated for crimes they did not commit.[93] According to the Innocence Project, there have been 232 post-conviction exonerations

[89] *See* source cited *supra* note 86.

[90] *Solving Cold Cases with DNA*, DNA INITIATIVE: ADVANCING CRIMINAL JUSTICE THROUGH DNA TECHNOLOGY, *available at* http://www.dna.gov/funding/cold_case/.

[91] *Id.*

[92] *See* Lynn Sweet*, Emmett Till Civil Rights Bill Passed by Senate. Names After Chicago Youth Murdered in Mississippi in 1955,* CHICAGO SUN-TIMES*,* Sept. 24, 2008*,* http://blogs.suntimes.com/sweet/2008/09/emmett_till_civil_rights_bill.html.

[93] U.S. DEPARTMENT OF JUSTICE ADVANCING JUSTICE THROUGH DNA TECHNOLOGY (2008), http://www.justice.gov/ag/dnapolicybooktoc.htm.

by DNA testing nationwide in thirty-three states.[94] For instance, in Nebraska, six individuals were wrongfully convicted of murder and were then exonerated by DNA evidence.[95] If DNA samples could have been taken at the time of arrest, there is a high probability that these individuals could have been proven innocent and thus avoided incarceration and possible death penalty.

In the case of cold cases from the Civil Rights era, there may have been some innocent people who were incarcerated or charged for crimes they did not commit. With the use of DNA technology, law enforcement may be able to clarify some of these issues.

2. Issues Raised by the Expansion of DNA Databases

Despite the positive outcomes that have resulted from the expansion of DNA and related databases, critics have argued that this expansion raises significant legal, ethical, and social issues, mostly related to privacy and civil liberties.[96]

a. Retention of DNA Samples by the Government

Privacy interest issues may arise when the government collection of DNA sampling is used to create a DNA profile that is then kept in a database, and searched repeatedly without the individual's approval or knowledge.[97] DNA samples contain personal information such as family relationships, disease susceptibility, physical attributes, genetic mutations, ancestry, and,

---

[94] Five Pardoned in Nebraska, Innocence Project, http://www.innocenceproject.org/Content/1806.php (Jan. 26, 2009, 18:10 EST).

[95] *See* State v. White, 740 N.W.2d 801 (Neb. 2007).

[96] Human Genome Project Information, DNA Forensics (2009), http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml.

[97] Dustin Hays & Sara Katsanis, *DNA, Forensics, and the Law*, GENETICS AND PUBLIC POLICY CENTER, July 24, 2007, http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42.

in the future, perhaps predilection to certain behavioral traits such as propensity to antisocial behavior.[98] Police, forensic science services, and researchers would all have access to people's DNA without their consent through the database.[99]

The inclusion of the samples in a national databank is currently not permitted by CODIS.[100] However, most states are silent or unclear on this issue.[101] Several states actually require that specimens be maintained.[102] Only one state, Wisconsin, requires the offender specimens to be destroyed after profiling.[103]

Once an individual's DNA sample is added to the federal database, critics argue, that the person will be treated as a suspect "every time a match with a crime-scene specimen is sought-even though there is no reason to believe that the person committed the crime."[104] This type of incident could occur with innocent people. For instance, if an individual had a similar profile to the person who actually committed the crime or if the individual happened to be at the crime

[98] *See* source cited *supra* note 96.

[99] *Id.*

[100] Hays & Katsanis, *supra* note 97; *see also*, 42 U.S.C §§ 14131-32 (1994). This statement was accurate at the time this article was written. For updated statistics, visit http://www.fbi.gov/hq/lab/codis/clickmap.htm.

[101] *Id.*; *see also* source cited *supra* note 96. This statement was accurate at the time this article was written. For updated statistics, visit http://www.fbi.gov/hq/lab/codis/clickmap.htm.

[102] *See supra* notes 96-97, 100 and accompanying text.

[103] WIS. STAT. § 165.771(3).

[104] Rick Weiss, *Vast DNA Pits Policing v. Privacy*, WASH. POST, June 3, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/02/AR2006060201648.html.

scene, the innocent would immediately be considered as "a suspect" because of the DNA sample retention policy.[105]

Critics claim that this retention of private information creates a possibility of privacy intrusion because genetic information can be easily found from DNA samples.[106] In their views, these databases are "starting to look more like a surveillance tool than a tool for criminal investigation."[107] Critics treat this retention as an intrusion of personal privacy and a violation of civil liberties, acts that are prohibited by the U.S. Constitution.[108]

b. Fourth Amendment

The primary purpose of the Fourth Amendment of the Constitution is to prohibit the government from exercising unreasonable searches and from intruding into the personal lives of its citizens.[109] The Fourth Amendment ensures "the right of people to be secure in their persons . . . against unreasonable searches and seizures."[110] A search is generally considered reasonable when it is supported by a warrant based on "probable cause", defined as a reasonable belief that a crime has been committed by the individual whose person on property is searched or seized.[111]

According to numerous U.S. Supreme Court decisions, the U.S. Courts have traditionally considered the collection and analysis of an individual's DNA to be an unreasonable "search" for

---

[105] *See* source cited *supra* note 96.

[106] *Id.*

[107] *See* source cited *supra* note 104.

[108] *See* source cited *supra* note 96.

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

[110] *Id.*

[111] Hays & Katsanis, *supra* note 97.

several reasons.[112] Among the reasons, one of them is bodily intrusion.[113] To collect a DNA sample, intrusion into the body is required, and this act is unreasonable.[114] Additionally, the "uniquely personalized nature" in the information contained in the DNA itself may constitute an unreasonable intrusion into the body.[115] The DNA sample contains sensitive and personal identification information.[116]

Despite these decisions, U.S. Courts have consistently supported "the operation of convicted-offender DNA databanks" for other reasons.[117] For instance, in *State v. Olivas*, the court stated that the government's interest is one of "special needs, beyond the normal need for law enforcement."[118] Moreover, in *Jones v. Murray*, the court stated that "with the person's loss of liberty upon arrest comes the loss of at least some, if not all, rights to personal privacy otherwise protected by the Fourth Amendment."[119] This statement in *Jones* means that when an individual is convicted, that individual immediately forfeits rights that he or she may otherwise

---

[112] *See generally* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 616 (1989); *see also* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[113] *Id.*

[114] *Id.*

[115] Simoncelli & Krimsky, *supra* note 28, at 4.

[116] *Id.*

[117] *Id.* at 3.

[118] State v. Olivas, 856 P.2d 1076, 1085, 1090 (Wash. 1993).

[119] Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992); s*ee also* Landry v. Att'y Gen., 709 N.E.2d 1085, 1092 (Mass. 1999).

have.[120] The *Jones* court reasoned that the DNA samples of convicted felons may be inserted into databanks because they have a diminished expectation of privacy.[121]

These court decisions indicate that the government may expand DNA and other related databases. Nevertheless, critics argue that some agencies and individuals that have access to databanks abuse their broad discretion.[122] Critics claim that that there is thus a high possibility that the databases are not used for criminal investigations purposes, but rather for other purposes and are misused.[123] Although it may be true that criminal defendants are often expected to give up some of their rights when they are convicted of crimes and sentenced to prison, critics argue that this cannot justify the right for the government to unlimitedly expand DNA databanks that are likely to violate individual rights guaranteed by the U.S. Constitution.[124]

c. Privacy – Family Searches

Due to similar patterns of DNA sequences among close family members, law enforcement may be able to determine whether a family member has committed a crime by comparing the DNA evidence left behind with another family member's DNA.[125]

---

[120] *Jones*, 962 F.2d at 312.

[121] *See generally id.* at 306.

[122] *See*, *e.g.*, Editorial, *DNA Testing for All Convicts*, CHI. TRIB., Jan. 29, 2002 (where, in relevant parts, "Defendants give up plenty of rights when they're convicted of crimes and sentenced to prison. Chief among them is freedom. They also lose much of their privacy. That's why a new statewide proposal to require that all convicted felons be required to submit a DNA sample shouldn't raise the hackles of civil libertarians or anyone else.")

[123] *Id.*

[124] *Id.*

[125] Hays & Katsanis, *supra* note 97.

Some of the methods used for familial searching involve "generating a list of possible relatives of the owner of DNA collected at a crime scene by performing either a 'low stringency' profile search to look for 'partial matches' between crime scene evidence and offender profiles or by conducting a 'rare allele' search."[126] Law enforcement officers are then able to locate close relatives and ask them for a voluntary DNA sample.[127]

If identified relatives refuse to provide a DNA sample, law enforcement may follow them and retrieve a discarded object, e.g., a coffee cup thrown away in a public trash receptacle, to compare the item's DNA trace with the DNA profile obtained at the crime scene.[128] Police have successfully extracted a suspects' DNA from articles such as discarded tissues, cigarette butts and envelopes.[129] Lower courts have held that there is "no reasonable expectation of privacy" in DNA that has been discarded.[130] Once an individual throws something in a garbage can, there is no reasonable expectation of privacy in that trash.[131]

Despite some courts' holdings that there is "no reasonable expectation of privacy" in DNA that has been discarded, critics argue that "involuntarily" discarded DNA contains highly personal information that should not be used in these circumstances.[132] Critics also claim that it

---

[126] Simoncelli & Krimsky, *supra* note 28, at 10.

[127] *Id.* at 11.

[128] *See* source cited *supra* note 96.

[129] *Id.*

[130] Commonwealth v. Ewing, 854 N.E.2d 993, 1001 (Mass. App. Ct. 2006).

[131] *Id.*; *see also* Hays & Katsanis, *supra* note 97.

[132] *Id.*; *see also* source cited *supra* note 96.

is unfair for the police to focus on these innocent people simply because of their familial ties.[133] This approach may reveal a genetic link between individuals who were not aware of their relationship with the suspect and lead to unexpected problems.[134] Even if this approach concerns some policy issues, proponents argue that these concerns outweigh the positive results, giving clues that could eventually help to solve crimes.[135]

d. Race

As previously stated, the FACES Lab and the Emmett Till Unsolved Civil Rights Crime Bill are working toward solving crimes using DNA and constructing a DNA database, which may be utilized to identify murders due to racism.[136] However, the use and expansion of DNA databases may bring contrary results. The Civil Rights movement of the 1960's decreased the significance of race and racial differences. But the newly developed DNA databases may actually deepen racial inequalities in the criminal justice system.[137] Also likely is the expansion of DNA databanks to bring back bad memories from the Civil Rights era.

In addition to the possibility of reopening wounds from the Civil Rights era, the expansion of DNA databanks may also increase the distrust of law enforcement by minorities.[138] Studies have shown that the "U.S. criminal justice system is fraught with racial disparities."[139]

---

[133] *See supra* notes 96, 130.

[134] *See* source cited *supra* note 96.

[135] *Id.*

[136] Anderson, *supra* note 51.

[137] *See* source cited *supra* note 96.

[138] *Id.*

[139] *Id.*

The studies have also demonstrated that non-whites are significantly more likely to be arrested than whites.[140] This means that a DNA database will contain a disproportionate number of minorities because of disparate arrest and conviction practices in the U.S.[141] Therefore, minorities will be more likely to be identified than whites upon comparing the profiles included in databases to the DNA evidence gathered from a crime scene.[142] Consequently, critics claim that the expansion and use of DNA databases will further deepen the racial inequalities in the criminal justice system.[143]

e. Quality of Laboratories

Forensic DNA and convicted DNA testing laboratories are required to comply with the National Quality Assurance Standards.[144] These standards were developed by the DNA Advisory Board (DAB) and issued by the Director of the FBI.[145]

Generally, courts consider DNA evidence to be reliable.[146] However, concerns about the accuracy and reliability of testing performed by some laboratories performing the forensic DNA analysis still exist.[147] Careless mistakes, sloppiness, or other errors that occur in laboratory

---

[140] *See* source cited *supra* note 96.

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] QUALITY ASSURANCE AUDIT FOR FORENSIC DNA AND CONVICTED OFFENDER DNA DATABASING LABORATORIES, FEDERAL BUREAU OF INVESTIGATION (2004), http://www.fbi.gov/hq/lab/fsc/backissu/july2004/pdfs/seubert.pdf

[145] *Id.*

[146] Hays & Katsanis, *supra* note 97.

[147] *Id.*

testing may result in injustice; for instance, an innocent person may be identified as the perpetrator.[148] If these errors were to occur in Civil Rights era cases, an innocent individual wrongfully convicted and his/her loved ones would face injustice, and the family members of the Civil Rights era victim would once again be wounded and would not find justice.

CONCLUSION

Although critics of the expansion of DNA databases claim that biological samples and DNA data can be misused if they are not controlled by the government, research has shown that indeed it helps law enforcement to solve crimes. For its crime solving efficiency, many people would not fault its continued use by law enforcement.

DNA forensic technology can probably be considered as one of the law enforcement's most outstanding tools in crime-fighting history. As examined in the discussion section of this note, DNA has been a tremendous resource for solving crimes that were once believed to be unsolvable.

The privacy concerns associated with potential misuse of DNA information can be safely handled by laboratories. Allowing research in law enforcement databanks and expansion of these databanks will not only help the United States to solve all criminal cases, from current to decades old cases from the Civil Rights era, but will also help the nation to become a safer place to live.

[148] Hays & Katsanis, *supra* note 97.

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 4, PAGE 79

Open Source or Open Season?: What legal professionals need to know about open source software before dealing in corporate transactions and the ramifications of GPLv3

Emily Prudente*

INTRODUCTION

Open source software, until recently, was a relatively unknown part of the landscape of software development. With the Internet's growing ubiquity and usage, the use of open source software increased and evolved rapidly. The unique licensing schemes covering open source software make it particularly intriguing from a legal perspective, and for uninformed legal professionals. Without an acute understanding of the details of these licenses the world of open source code quickly becomes treacherous and ripe with potential pitfalls. Open source licensing creates liabilities and with its overwhelming benefits and increasing acclaim, this new software is impossible to ignore.

Software developers and copyright holders have begun to turn to the courts for guidance on the degree of recognition and level of protection they can expect from the judicial system.[1] Recently, there have been a number of actions addressing the enforceability of open source licenses.[2] While most suits have settled, there has been important litigation that suggests how the legal system is likely to analyze cases involving these licenses.

---

* J.D. candidate, Syracuse University College of Law, expected 2010; Lead Articles Editor, *Syracuse Science & Technology Law Reporter*.

[1] Rachel Stern & Erik C. Kane, *Open For Business: What Corporate Counsel Need to Know in the Intricate World of Open Source Code*, ACC DOCKET 26 NO. 10, 46 (2008).

In the context of mergers and acquisitions, recognition and management of open source code is critical for a number of reasons. The presence of open source can affect the value of a company's intellectual property assets, thereby affecting the value of the deal itself.[3] The risk of lawsuits and lost revenue increases when upper management or in-house legal counsels are not kept abreast of the type of licenses that may be intertwined with their proprietary software.[4] For attorneys practicing corporate law, intellectual property law, or those who serve as general counsel to technology companies, awareness of the increasingly complex world of open source licensing is of paramount importance.[5] Companies stand to lose a great deal, in some cases, everything, if open source code is not properly managed. Despite the risks, however, open source software has established itself as an intangible asset companies can no longer afford to ignore and whose benefits far outweigh the risks.

Understanding the Basics of Open Source Software

A solid understanding of open source software is crucial to properly manage it.[6] To appreciate the value of open source software, it is helpful to begin by understanding the basics of computer software. The term "software" refers in general to computer programs that function to operate the computers and run various and sundry devices related to computers.[7] Common

---

[2] Jacobsen v. Katzer, 609 F.Supp.2d 925, 928 (N.D. Cal. 2009).

[3] Alan Stern, *Open Source Licensing*, Practising Law Institute: Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 915 PLI/Pat 187, 196 (2007).

[4] *Id.*

[5] *Id.*

[6] Stern & Kane, *supra* note 1, at 42.

[7] Dr. Jose J. Gonzalez de Alaiza Cardona, *Open Source, Free Software and Contractual Issues*, 15 TEX. INTELL. PROP. L.J. 157, 162 (2007) [hereinafter Gonzalez].

practice among software engineers is to write programs in easily interpretable computer programming languages, such as C++ and Java.[8] When programs are written in these languages the resulting source code is comprehensible to programmers and engineers, but not to machines.[9] In order to execute a program the computer must translate the source code into what is known as object code, or binary code.[10] After translation, the source code is a series of 1's and 0's that only machines can interpret.[11] In the interest of maintaining and protecting trade secrets, engineers frequently deliver programs in object code form.[12] Reverse-engineering source code from object code is so difficult it is effectively impossible, with the result that if a program has been delivered in binary form, there is no reasonable probability that purchasers will uncover the underlying source code.[13]

Protection of proprietary code, particularly for companies that derive significant portions of revenue from their intellectual property assets, is vital to advance and thrive in their respective fields. If software is delivered by the developer in source code form, the company becomes vulnerable to disclosure of their trade secrets and exposure of its intangible intellectual property assets it has spent substantial time and money developing.[14] In instances such as these, a firm's intellectual property may be the cornerstone of its competitive advantage in the marketplace.

---

[8] Stern & Kane, *supra* note 1, at 42.

[9] Gonzalez, *supra* note 7, at 163.

[10] *Id.*

[11] *Id.*

[12] *Id.* at 164.

[13] *Id.*

[14] Stern & Kane, *supra* note 1, at 43.

But while protecting trade secrets can be critical to a company's survival, it comes at a price. The obvious goal of developing software for sale or license is to generate revenue by providing solutions that competitors are not able to offer to the market. In accomplishing this goal software is developed by engineers in all companies in an environment that promotes secrecy instead of in an atmosphere that encourages the sharing of ideas between developers. The philosophy of open source software is to overcome corporate barriers of secrecy in order to foster innovation more rapidly and efficiently among developers at different companies who share common programming goals.[15]

The concept of synergy is a pillar in the philosophy of open source code; the more mind-power devoted toward a common goal, the richer and more robust the end-product will be. In the eyes of those who are involved in the movement, the resulting whole can in fact be greater than the sum of its parts.

A number of forces have facilitated the movement for sharing open source code. Due to its increasing use and development, the internet serves as an excellent medium through which code can be more readily accessed and shared among peers.[16] Supporters of the open source software movement encourage sharing ideas and improvements when open source is made available to a community of peers. This support forms the foundation of the open source philosophy.[17] Also, there is the cost-effective benefit to using open source code because it is less expensive than proprietary, closed source code.[18] Free access to programmers' work product

---

[15] *Open Source Definition: Annotated*, Open Source Initiative, http://www.opensource.org/docs/definition.php.

[16] Stern & Kane, *supra* note 1, at 42.

[17] *See* source cited *supra* note 15.

provides programmers with the opportunity to incorporate their ideas into new program while allowing others to improve the code without the financial burden of licensing fees or royalties.[19] Of course, this depends in part on the license under which the source code is covered. These licenses will be discussed and analyzed in detail later in this paper.

Open Source Initiative (OSI)

The open source movement began decades ago and evolved from what was originally called the free software movement, which Richard Stallman began.[20] A brief discussion of free software is necessary to appreciate the subtle differences between free and open source software.[21] A common misconception is that free software is "free of charge." This is not true. The free software movement emphasizes the freedom to replicate, adapt and subsequently redistribute the work.[22] On the other hand, the open source movement emphasizes access to the source code but not necessarily the ability to modify and/or redistribute the program.[23] At first impression the open source philosophy may appear to run counter to the goal of most corporations to generate a profit. Bill Gates, a well-known opponent of open source posited, "One thing you do [when implementing open source philosophies] is prevent good software from being written. Who can afford to do professional work for nothing?"[24] Programmers who

---

[18] Gonzalez, *supra* note 7, at 171.

[19] Stern & Kane, *supra* note 1, at 42.

[20] *Id.*

[21] Gonzalez, *supra* note 7, at 167.

[22] Matt Lee, *What is Free Software and Why is it so Important for Society?*, FREE SOFTWARE FOUNDATION, March 29, 2010, http://www.fsf.org/about/what-is-free-software.

[23] Gonzalez, *supra* note 7, at 180.

participate in the open source movement are typically motivated by goals other than direct economic gain.[25] There is satisfaction and prestige in creating or modifying a program, and also the possibility of economic benefit from sources other than copyright.[26] The open source software movement is premised in part on the idea that with plentiful beta-testing[27] and with enough sets of eyes, any program can be improved and de-bugged.[28] Such a community-based approach, therefore, increases efficiency in the software development market.[29]

The open source, as opposed to free software, movement officially began in 1998 when Netscape announced it would release the source code for its popular internet browser.[30] The Open Source Initiative (OSI) was formed by a group of scientists whose goal was to make the open source concept attractive to the corporate world.[31] While some free software enthusiasts, such Linux creator, Linus Torvalds, support the open source movement, others like Richard Stallman, do not.[32]

---

[24] Gonzalez, *supra* note 7, at 177.

[25] *Id.* at 175.

[26] *Id.*

[27] The concept of beta-testing refers to the common practice of software engineers to trial, typically in-house, a version of their code before releasing the program for use either internally or for external customers. Essentially, it is a quality control mechanism that offers some assurance of reliability for a brand new product.

[28] Gonzalez, *supra* note 7, at 176.

[29] *Id.*

[30] *Id.* at 178.

[31] *Id.*

[32] *Id.* at 179.

Prevalence of Open Source

There are successful for-profit corporations whose business models are built around open source, such as Red Hat.[33] Red Hat is famous because it is built on the model of "media distribution, branding, training, consulting, custom development, and post-sales support" and delivers both software and maintenance support for its patrons.[34] Many products based in full or in part on open source code are increasing in prevalence. For example, almost 70% of web servers are run by Apache, an open source software package.[35] Many domain name servers, like Mozilla's Firefox, implement BIND which is another open source package.[36] Outside the cyber-world, antilock brakes, watches, mobile phones, PDAs, television set-top boxes, and medical equipment are just a few of the electronic devices that incorporate open source software.[37] The open source Linux operating system, based on open source code, has roughly 29 million users.[38] This market share is dwarfed by the number of users of the widely-known Microsoft Windows operating system.[39]

The GPL

Of all the licenses covering open source products and services, the most popular is the General Public License, or, commonly, the GPL. Linux, Playstations 2 and 3 and some cell

---

[33] Gonzalez, *supra* note 7, at 177.

[34] *Id.*

[35] *Id.* at 160.

[36] *Id.*

[37] *Id.* at 161.

[38] Gonzalez, *supra* note 7, at 161.

[39] *Id*.

phone carriers all are licensed under the GPL version 2, which, until recently, was the newest version.[40] The idea for a general public license emerged from the difficulties inherent in placing computer programs in the public domain. Allowing access to open source software without any legal structure would lead to complications that would effectively frustrate the community-oriented goals of free software.[41] For example, programs in the public domain may be released in object code form.[42] Also, without licensing restrictions, even those programs released in source code could be redistributed only as object code.[43] Releasing programs in object code format prevents downstream users from accessing, adapting or redistributing the program. This format interferes with the sharing of the ideas, and that concept is central to the open source philosophy.[44]

The GPL, also called the GNU GPL, is issued to the majority of users of open source software.[45] The license has two primary clauses. The first grants users the right to access, modify and redistribute the source code. The second requires that redistribution be performed under the same terms as those of the license that gave permission to access, modify and redistribute the code.[46] This second part is known as the "free software clause" or "copyleft clause" because it permits redistribution without authorization and thus denies the creator one of

---

[40] Stern & Kane, *supra* note 1, at 42.

[41] *See* source cited *supra* note 22.

[42] Gonzalez, *supra* note 7, at 173.

[43] *Id.*

[44] *See* source cited *supra* note 15.

[45] *Id.*

[46] GNU General Public License, version 2 (2001), http://www.gnu.org/licenses/old-licenses/gpl-2.0.html#SEC3.

the exclusive rights held by copyright owners, the right to distribute.[47] The GPL is rendered truly complex and unusual by the inclusion of the copyleft clause.[48] The perpetual nature of the freedom to alter software by downstream developers gives the GPL a viral, reciprocal, or hereditary, characteristic.[49]

The significance of the copyleft clause is that any open source program, whether modified or not, must be redistributed to downstream users with permission to access and modify the code.[50] Copyleft licenses impose an obligation on downstream licensees to redistribute their respective programs – modified or not – under the same copyleft clause.[51] This treatment of modified software that has been redistributed is the critical difference between open source licenses and proprietary commercial licenses.[52] It is illustrated by a comparison of two of the most notable open source licenses: the GPL and Berkeley Software Distribution (BSD).[53]

---

[47] The GPL states, "You may convey a work based on the Program, or the modification to produce it from the Program, in the form of source code . . . provided that . . . c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply . . . to the whole of the work, and all its parts, regardless of how they are packaged." GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

[48] Sapna Kumar, *Enforcing the GNU GPL*, 1 J. L. TECH. & POL'Y 1, 11 (2006).

[49] Ira Heffan, *'License Compatibility' in Open Source Licenses*, Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 916 PLI/Pat 11, 16 (2007).

[50] Gonzalez, *supra* note 7, at 173.

[51] *Id.* at 185.

[52] Matthew A. Neco and Wendy Millar Goodkin, *Free and Open Source Software: Risks Your Company's Software Developers Might Not Be Aware Of*, in UNDERSTANDING OPEN SOURCE SOFTWARE, *available at* http://www.acc.com/resource/v6861. *See also* Stern & Kane, *supra* note 1, at 43.

[53] Stern & Kane, *supra* note 1, at 43.

Berkeley Software Distribution (BSD) and other Permissive Licenses

The Open Source Initiative (OSI) sets forth ten requirements for a license to receive recognition for complying with the OSI's principles. They include the right to free distribution, accessibility of underlying source code, possession of the option and capability to revise derivative works, protection of the integrity of the original author's code, no discrimination against individuals or groups, distribution of the license with all subsequent works derived in whole or in part from others' code, prohibition of restrictions on other software, and finally, the license must be "technology neutral."[54] The OSI website provides descriptive details for each of the ten principles.[55]

Some open source licenses permit the free sharing of source code among developers without requiring them to make public and to license forward their innovations and modified versions of the software.[56] These licenses are referred to as permissive or "non-copyleft" licenses.[57] Unlike the GPL licenses, these permissive licenses do not contain copyleft clauses. Examples include the Berkeley Software Distribution (BSD) license, Apache, and others.[58] These licenses differ from hereditary licenses primarily in their treatment of programmers' ability to limit access to the derivative works created from the initial open source code. The BSD license, for example, permits free software to be turned into proprietary software without requiring that the derivative work be redistributed under the original license.

---

[54] *See* source cited *supra* note 15.

[55] *Id*.

[56] Stern, *supra* note 3, at 218.

[57] *Id.*

[58] *Id.* at 214-15.

General Public License Version Three (GPLv3)

Version 3 of the General Public License was released at the end of June 2007.[59] While its release was a monumental event for the software community, it was overshadowed by the release of Apple's iPhone on the very same day.[60] Generally, version 3 reflects the philosophy and values of the open source community.[61] Typically the parties involved when dealing with open source products include the vendors, contractors, and customers.[62] Breaching the GPL becomes most pressing when the software is distributed to third parties and so for obvious reasons, it is important to understand the key elements of the license.[63] In the business world, these parties are typically acquirers (those organizations or companies looking to buy another business entity), targets (those entities being evaluated by acquirers to become part of the acquiring company's organization), and customers (meaning the consumers – either individuals or business – that serve to generate revenue for a business organization). Because of the high risk of subsequent lawsuits and publicity debacles if open source code is improperly handled, many customers, potential partners, and potential acquirers are demanding indemnification clauses at the outset of a deal.[64]

---

[59] Stephen J. Davidson & Nathan S. Kumagai, *Developments in the Open Source Community and the Impact of the Release of GPLv3*, Practising Law Institute: Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 929 PLI/Pat 319, 325 (2008).

[60] *Id.*

[61] *Id.* at 327.

[62] Stern, *supra* note 3, at 192.

[63] *Id.*

[64] *Id.*

There are five notable revisions in GPLv3 of which corporate attorneys, in-house counsel, and intellectual property lawyers should be aware. First, version 3 permits software distributors to restrict, but not eliminate, the effect patents have on redistribution use of open source programs.[65] This is accomplished in section 11 of the license by explicitly offering a patent grant and then defining it so there is no room for ambiguity when the license is executed.[66] "Patent license" is defined as "any express agreement or commitment…not to enforce a patent."[67] Version 2 was much stricter regarding the intersection of software patents and the GPL.[68] In fact, the preamble states, "we wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all."[69]

The next notable clause addresses "cross-licensing" agreements.[70] These agreements apply to both users who are parties to the agreements and users who are not parties to the

---

[65] From Section 11 of GPLv3: "Each contributor grants . . . a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version." GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

[66] *See id.*

[67] *Id.*

[68] GNU General Public License, version 2 (1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt.

[69] *Id.*

[70] Stern From Section 10 of GPLv3: "Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License….If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever

agreements.[71] The language in GPLv3 addressing these agreements essentially states that the licensor and licensee agree not to sue each other for software patent infringement.[72] This condition was absent in version 2.[73] The decision to include this new provision is a direct result of the conflict between Microsoft and Novell in which the former agreed not to enforce its patents against the latter's SuSE Linux customers.[74]

Tivo-ization refers to the practice of employing software licensed under the GPL in a hardware device (such as the popular TiVo digital video recorder used to record television programs) thereby preventing users from sharing the underlying source code.[75] This is a blatant violation of the open source philosophy's freedom to retain, share and allow access to source code. Tivo-ization thus undermines this important goal of the open source movement.[76] The third revision addresses this issue.[77] Version 3 added a clause to ensure open source works under

---

licenses to the work the party's predecessor in interest had or could give[.]" GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

[71] *See supra* note 70 and accompanying text.

[72] Davidson & Kumagai, *supra* note 59, at 199.

[73] GNU General Public License, version 2 (1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt.

[74] Microsoft provided a license for its intellectual property directly to the end user rather than the developer (Novell). For details on this controversy, *see* Tom Sanders, *Microsoft Signs Up LG for Linux Patent Deal*, V3, Jun. 8, 2007, http://www.vnunet.com/vnunet/news/2191649/microsoft-signs-lg-linux-patent.

[75] *An Introduction to Tivoization*, The Linux Information Project, http://www.linfo.org/tivoization.html (last visited May 11, 2010).

[76] *Id.*

[77] GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

the GPL which will continue to permit future downstream modifications.[78] It is known as the "anti-tivo-ization" clause.[79] Section 1 of version 3 requires licenses to provide "complete and corresponding source" code which includes instructions and information sufficient for a user to execute modified versions of the software. [80] Those most affected by this clause are distributors of devices like TiVo, because the clause does not permit modified code version to run in those distributors' products.[81]

Version 3 goes beyond previous versions of the GPL by not only identifying when covered works must be licensed under the GPL, but by also identifying when derivative works must be licensed.[82] This is a significant modification to the license because despite the self-perpetuating nature of the GPL, the change articulates circumstances in which a work derived under a hereditary license does not necessarily self-perpetuate in a manner detrimental to the copyright of works aggregated with it.[83] [84]

---

[78] GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

[79] Stern, *supra* note 3, at 223.

[80] "If you convey an object code work under this section in, or specifically for use in, a [consumer] Product . . . the Corresponding Source conveyed . . . must be accompanied by the Installation Information . . . Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documents (and with implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying." GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html (referring to § 6 specifically).

[81] Stern, *supra* note 3, at 223.

[82] Stern & Kane, *supra* note 1, at 44.

[83] Heffan, *supra* note 49, at 16.

[84] "A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an

Finally, the definition of "corresponding source" is included in the text of the license so that licensees are aware that incorporated and/or copied code is defined to include code used to modify, install and run programs.[85] Version 2 addressed corresponding source code in its section 3(b), but included no description or definition of it, thus causing confusion for users.[86]

The new version of the GPL has not been well received by the entire open source community. Linus Torvalds, a well-known GPL supporter and open source enthusiast, has made his acceptance of version 3 contingent upon Sun Microsystems' release of Solaris under GPLv3.[87] He cites as his concerns interference with hardware and software, and he questions the appropriateness of some revisions. On the other hand, GPLv3 has received strong support from the Samba Project, Free Software Foundation, IBM and Sun Microsystems. How it will ultimately be received by the open source community remains to be seen.

'aggregate' if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate." GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html (referring to § 5 specifically).

[85] "The 'Corresponding Source' for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities . . . The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source. The Corresponding Source for a work in source code form is that same work." GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html (referring to § 1 specifically).

[86] GNU General Public License, version 2 (1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt.

[87] Davidson & Kumagai, *supra* note 59, at 142.

Compatibility issues between licenses

With the variety of open source code licenses available, compatibility problems have arisen.[88] These complications are more related to the legal provisions in the licenses, more so than technical compatibility issues.[89] Because of these difficulties the ways in which code from multiple sources may be properly combined under the terms of the licenses are limited.[90] Perhaps the most remarkable consequence of the incompatibility is that two sets of source code licensed under reciprocal, or hereditary, licenses could not be combined under another reciprocal license.[91] This is because each license would require the resulting work be covered under a license identical to itself.[92] Code covered under the GPL is included in this licensing conundrum. To be compatible with the GPL, the license must contain a clause embodying the spirit of the copyleft clause from the original GPL.[93] For example, if a GPL product were combined with a product covered under the Artistic License (another copyleft, or hereditary, open source license), each license would require that the derivative program be licensed under its own terms. This is a complicated and grave legal problem if the code under these respective licenses became co-mingled post-merger or acquisition. Fortunately, the new GPLv3 resolves

---

[88] *Open Source Licenses By Category*, Open Source Initiative, http://www.opensource.org/licenses/category. Click on any link for the various categories of licenses and it becomes readily apparent that there is great variety in conditions and requirements for each category of open source license.

[89] *Id.*

[90] Stern & Kane, *supra* note 1, at 44.

[91] *See* GNU General Public License, version 2 (1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt; *see also Artistic License 2.0*, Open Source Initiative, http://www.opensource.org/licenses/artistic-license-2.0.php.

[92] *See* sources cited *supra* note 91.

[93] *Id.*

this quandary by providing that open source covered under it or a similar reciprocal (hereditary) license may be combined with code covered by a non-reciprocal license.[94]

Another example of incompatibility between licenses arises where a derivative work contains code covered by a permissive license such as the BSD and also contains code covered by the GPL. The BSD terms are more permissive than those of the GPL, meaning the license does not require a derivative work to be licensed under the BSD itself. This is one of the reasons it is popular among commercial software developers. However, when work covered under a license similar to the BSD is combined or commingled with work covered under a GPL version 2, the work must be subsequently licensed under the GPL, and not the BSD.[95] The GPL's requirements that a derivative work be covered under the same license as the original work would be violated if the BSD license were used instead.

From a corporate transactions perspective, not only must attorneys determine whether open source code has been used in a target company's software, but must also determine under what license the code was licensed to the target company. Additionally, it is crucial that legal professionals representing corporations or intellectual property based companies ascertain whether that code is going to be combined with any existing software of a potential acquiring company, and whether the acquiring company's software may be combined with the target company's code.[96] In short, it is critical that legal professionals consider the possibility of incompatible licenses if open source code is to be combined with other code in existing products and licensed further.

---

[94] GNU General Public License, version 3 (2007), http://www.gnu.org/copyleft/gpl.html.

[95] *See* sources cited *supra* note 91.

[96] Stern & Kane, *supra* note 1, at 45.

Acquisitions and the Corporate Context

Products incorporating open source code are proliferating exponentially whether the software developers are aware of its presence or not.[97] Many businesses operate in a "mixed-IP environment." These environments contain many types of programs licensed under many disparate licenses, each with specific provisions, conditions, and prohibitions. As a result, it is becoming more common for new software to be created by using as its building blocks prior pieces of work.[98] Layering of code creates a melting pot of software owned by the developer with code owned by someone else, some of which is likely to be open source.[99] It is unsafe to assume that corporate software engineers are aware of the implications of open source licenses, particularly the reciprocal nature of the commonly used GPL.[100] Since decisions to include open source code in proprietary software are not necessarily made by chief engineers or product managers, management may not be aware of the degree to which open source code is being incorporated into software in most companies.[101] It is critical to ascertain the extent of the use of open source code in any company.[102]

---

[97] Stern, *supra* note 3, at 191.

[98] Kat McCabe, *Working with Open Source: Software Compliance Management*, Practising Law Institute: Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 927 PLI/Pat 473, 477 (2008).

[99] *Id.*

[100] Stern, *supra* note 3, at 191.

[101] *Id.*

[102] McCabe, *supra* note 98, at 477.

Knowing the value of a target's intangible software assets or of its utility for a given purpose is insufficient for proper conduction of a deal valuation.[103] The target's rights to its intellectual property must be ascertained and, quite likely, this will entail tracing the software's development from a legal perspective.[104] It is not difficult to foresee a scenario where, if a target's intellectual property assets are inaccurately valued, the perceived value of the deal will likely be inaccurate as well.[105] The less exclusive the rights a company has to its intellectual property assets, the less that company's value is.[106] The results of a miscalculated valuation of a corporate transaction may include unanticipated competition from other rightful owners and users of the assets, or, if the assets that were once proprietary have lost their exclusivity due to mismanagement of licensing rights, there may be no value to the intellectual property assets at all.[107] Clearly, these results are undesirable but given the proper training and information, savvy legal professionals will be well-equipped to manage open source licensing issues.

Valuation of a prospective acquisition becomes more critical when a sizeable percentage of a company's assets are composed of intellectual property.[108] Potential purchasers should identify the scope and value of a target's intellectual property assets so as not to over-pay for the

---

[103] Anthony F. Lo Cicero et al., *Acquiring or Selling the Privately Held Company 2008*, 1675 PLI/Corp 733, 739 (2008).

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] Lo Cicero, *supra* note 103, at 737.

acquisition, and in order to maximize the value of those assets after the transaction.[109] Licensed intellectual property rights are not necessarily transferable by the licensee without express permission by the licensor, thus decreasing the value of the licensee's rights to the asset.[110] The desirability of the target of an acquisition may or may not stem largely from its intellectual property. Either way, mismanagement of open source code can derail a deal or devalue a company very quickly. If a target's cornerstone products serve as the main attraction and impetus for the deal, and those products were developed by software engineers through the use of open source code, it does not take much of a leap to see how quickly the company could be devalued in the eyes of the potential purchaser, and the deal itself placed in jeopardy.[111] The risk of lawsuits and the potential for unfavorable publicity may also discourage other companies considering entering into a bidding war with the known suitor for the target and so market competition and efficiency are diminished.[112] For obvious reasons, due diligence with respect to assessing intellectual property assets has become a prominent concern and at the forefront of the minds of savvy corporate, in-house, and intellectual property attorneys.[113]

Some executives or product managers might prefer the "ignorance is bliss" approach when it comes to licensing structures.[114] Quite frankly, it is often less expensive for businesses to build new software based on previous works, whether those works are for internal use at the

[109] Lo Cicero, *supra* note 103, at 739.

[110] *Id.* at 737.

[111] Stern, *supra* note 3, at 194.

[112] *Id.*

[113] *Id.*

[114] Stern & Kane, *supra* note 1, at 46.

company that employs the developers, or for external use whereby the company will pass the work to outside parties for profit.[115] Open source is almost always seen as a less expensive alternative to proprietary assets.[116] Time and development costs are reduced while quality assurance and reliability are potentially increased.[117]

It is tempting for upper management to address problems that appear simple to resolve, that are quickly fixable and manageable, rather than those that are tedious, difficult and less likely to be resolved with ease.[118] It is simply part of human nature to first deal with what is easily and readily fixable. Corporate entities have an enormous interest in identifying whether open source software may be present and if so, how it is being used and managed. Thus, extensive due diligence should be conducted prior to the acquisition of another company's intellectual property assets.[119] When forming strategic alliances, potential partners are currently demanding higher levels of assurance regarding intellectual property assets.[120] Investors and customers do not wish to be unpleasantly surprised to learn that a business may be vulnerable to lawsuits or loss of competitive advantage because of mismanagement of open source code.[121] This holds true for employees as well.[122]

---

[115] McCabe, *supra* note 98, at 477.

[116] Lo Cicero, *supra* note 103, at 755.

[117] McCabe, *supra* note 98, at 477.

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] McCabe, *supra* note 98, at 477.

Software Compliance Management and Due Diligence

Open source code carries with it serious risks that must be addressed before reaping the benefits of employing such software. It is remarkably easy to "license in" a publicity or legal nightmare.[123] In the corporate context and particularly where an acquisition is involved, it is necessary to understand that the identification of open source and compliance with license requirements is absolutely critical to the success of the deal and the survival of the parties involved.[124]

So where should a company begin? The appropriate standard of care is for the business to conduct due diligence. This entails a proper assessment of what a target is worth, what the value of its liabilities may be, will likely require a pre-acquisition audit of intellectual property assets.[125] Companies should begin by assessing the assets they are acquiring.[126] There are numerous rationales behind this including making sure the internal review is not unnecessarily complicated by the procedures used. A great deal of learning is likely to occur during the review process and it is easier to educate employees as opposed to third parties.[127] That is probably due to the simple fact that employees are on the premises and are easier to reach than outside parties. The goals of accurate asset valuation and identification are shared by all businesses that find themselves going through the major undertaking of a merger or acquisition.[128]

---

[123] Stern, *supra* note 3, at 192.

[124] Stern & Kane, *supra* note 1, at 42.

[125] Lo Cicero, *supra* note 103, at 738.

[126] McCabe, *supra* note 98, at 479.

[127] *Id.*

[128] *Id.* at 478.

Due diligence conducted when open source is at issue is not necessarily different from due diligence conducted for any other reason.[129] When managing open source both internally and during the acquisition of a target, a company's goals should include maintenance of continuity in its business model and compliance with legal obligations.[130] Checklists, drafts of representations and warranties, oral interviews all facilitate the process of due diligence.[131] External forensic computer consultants who specialize in programming may be hired to peel back the code layer by layer to determine whether open source might be present.[132] For example, Black Duck and Palamida are two companies that specialize in and provide such services in this arena.[133] Internal engineers can also be used to scrutinize code for any potential signs or indicators of open source in the assets.[134]

It is not hard to understand why a new field known as Software Compliance Management has emerged.[135] Its purpose is to offer guidance and facilitate transactions and manage internal assets.[136] Generally, Software Compliance Management can be understood to mean personnel or divisions that perform the function of, or the process of:

---

[129] McCabe, *supra* note 98, at 479.

[130] *Id.* at 478.

[131] *Id.* at 479.

[132] *Id.*

[133] Stephen J. Davidson & Nathan Kumagai, *Developments in the Open Source Community and the Impact of the Release of GPLv3*, Practising Law Institute: Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 916 PLI/Pat 121, 141 (2007); *see also generally* http://www.palamida.com and http://www.blackducksoftware.com.

[134] McCabe, *supra* note 98, at 479.

[135] *Id.* at 478.

- "Knowing what is in the code base and controlling the introduction of licensed materials into the code base;
- Knowing what obligations are related to the use of licensed materials, knowing whether the license obligations for combined components are compatible, and managing fulfillment of those obligations; and
- Managing this process from the product architecture all the way through deployment or distribution."[137]

Software Compliance Management provides assurance that the company's objectives are achieved and licensing obligations are complied with when using or incorporating new intellectual property assets.[138] An important consideration is whether the software licenses are assignable.[139] The purchaser should determine whether the target has received requests from rights owners for licenses and for the payment of licensing.[140] The Sarbanes-Oxley Act of 2002 was enacted as a corporate governance measure and is relevant to a discussion of performing due diligence.[141] Sarbanes-Oxley includes intellectual property assets under the company assets that must be monitored regularly.[142] Any existing impairments to a company's intellectual property assets must be disclosed.[143] If open source code is used improperly it can significantly damage an intellectual property asset. Sarbanes-Oxley compliance attorneys should communicate openly

---

[136] McCabe, *supra* note 98, at 478.

[137] *Id.*

[138] *Id.*

[139] Lo Cicero, *supra* note 103, at 754-55.

[140] Stern, *supra* note 3, at 194.

[141] *See* Sarbanes-Oxley Act of 2002 § 7202, Pub. L. No. 107-204, 116 Stat. 745 (2002).

[142] *Id.*

[143] *Id.*

with corporate finance departments to develop auditing procedures and ensure proper drafting of the certification.[144]

Certain problems are commonly faced by acquiring companies when open source software is involved. First, the improvements made to the open source code may be required to be publicized to the open source community depending on the requirements of the applicable licenses. Also, combining proprietary code with open source code could potentially render all the company's commercial and proprietary products subject to an open source license. Companies fearful of infecting their proprietary software with hereditary-licensed open source code may have the option of distributing the derivative work under a fee-based commercial license.[145]

Remediation

Despite all we know about open source and its exponential growth we have witnessed, there remain unanswered questions as to how to best track it and achieve compliance with relevant business standards and laws. Such questions include ascertaining the factors needed to conclude that copied work is *de minimus*, when do functions and expressions merge to the degree that we are no longer examining copyrightable code, and what is the responsible depth of investigation before accepting a developer's representation that the code was not wrongfully copied?[146]

Remediation is the next step in the open source management project following the performance of due diligence and can be considered the most challenging stage of the

[144] Stern & Kane, *supra* note 1, at 46.

[145] Stern, *supra* note 3, at 196.

[146] McCabe, *supra* note 98, at 480.

assessment.[147] Remediation refers to the process by which an entity can correct prior mistakes and perform damage control if necessary. Attorneys without extensive technical knowledge or background would be remiss if they did not consult with outside counsel who possesses the expertise to communicate directly with developers regarding remediation options and procedures.[148] The professionals consulted should be familiar with open source, cognizant of its development, know where to retrieve valuable information if needed, and ideally, have personal contacts in the open source community that could be consulted further.[149]

It is critical that there be open channels of communication among the attorneys involved in remediation, the management and the developers.[150] Sometimes companies will consent to specifics of a remediation plan of action and even secure their positions using escrow or holdbacks.[151] Failures or problems revealed by due diligence reviews vary in degree of seriousness and remediation procedures should be adjusted according to the severity of the problem.[152] Remediation costs and procedures may present formidable, challenging decisions for the company.[153] If compliance management inspection revealed that remediation can be achieved through replacement of noncritical code, many companies remain comfortable in

[147] McCabe, *supra* note 98, at 480.

[148] *Id.* at 484.

[149] *Id.*

[150] *Id.*

[151] *Id.* at 480.

[152] McCabe, *supra* note 98, at 480-81.

[153] *Id.* at 480.

proceeding with the transaction.[154] Often the remediation efforts will be left to the acquiring entity.[155] Unfortunately there are cases where inspections have uncovered serious circumstances of non-compliance.[156] If efforts to meet the necessary compliance standards failed, it can become challenging compromise on which entity (the target or the acquirer) will bear the costs of remediation.[157] It is likely the deal will be delayed as a result of having to conduct remediation procedures.[158] Where a deal is on the line and problems are identified, the best case scenario for complex remediation procedures is that the transaction will be delayed.[159] The worst case scenario would be for the acquirer to lower the price they are willing to pay or to cancel the deal in its entirety.[160] It is preferable for a company to voluntarily perform a due diligence review prior to having one forced upon it – substantial value and opportunity can potentially be lost if the latter occurs.[161]

The degree of sensitivity an acquiring company will have towards open source code depends in large part on the intended use of the software.[162] If the acquisition's purpose is to temporarily fill a hole in the acquiring company's product line, and the target's assets are

---

[154] McCabe, *supra* note 98, at 480.

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] McCabe, *supra* note 98, at 480.

[160] *Id.*

[161] *Id.*

[162] *Id.* at 481.

intended to remain as part of the subsidiary and not be rolled up into the parent, there may be relatively little sensitivity to problems that might be disclosed through extensive due diligence. The intent, or end-goal, of the corporate transaction may be for the acquired code to be replaced in its entirety by code developed as an integral part of the company's existing product line. This is not an ideal valuation scenario for the target company, but it will result in less need for code scans or other methods of detailed due diligence review. Whatever the acquiring company's motivation, if the intention is to merge the acquired code into the acquiring company's existing product line and combine it with other valuable software assets, then the sensitivity will be much higher and the discovery of even minor problems may be sufficient to tip the balance toward 'make' in a 'make versus buy' analysis.[163] During a merger or acquisition, depending on what the goals of the acquiring company are, if the acquiring company intends to replace its target's software with whatever the acquirer has developed internally, the acquirer will be more likely to continue to manufacture its software in-house and not pay additional cost, or pay a lower cost to acquire the intellectual property assets of the target. Contrarily, if the acquiring company seeks to replace or commingle its programs with those of the target, the price of the deal may increase because of the associated due diligence and potential remediation costs.

Enforceability of Open Source Licenses and Litigation

Traditionally, the failure to adequately investigate the use of open source code has not been in the forefront of legal professionals' concerns.[164] Until recently, there were no developers in a position to instigate any type of infringement action.[165] This relaxed attitude toward

[163] McCabe, *supra* note 98, at 481.

[164] Stern & Kane, *supra* note 1, at 46.

[165] *Id.*

compliance with open source licenses is likely to change in light of recent developments in litigation centering around the enforceability of open source licenses.[166]

Most strikingly, the U.S. Court of Appeals for the Federal Circuit recently found in favor of a copyright holder in the case of *Jacobsen v. Katzer*.[167] The outcome of this action addressing open source license enforceability was the reversal of the lower court's denial of a preliminary injunction. In *Jacobsen* the court held that plaintiff, who had created software used in conjunction with model trains and which was covered under the Artistic License (a hereditary, or viral, license similar to the GPL), was entitled to make a claim not only for violation of the license, but also for copyright infringement. Additionally he was granted the option to enjoin the defendants who copied the licensed software without adhering to the conditions set forth in the Artistic license. Certain features of the license, such as those ensuring access and the ability to modify code, as well as the requirement to make attribution to the author, were found to establish conditions limiting the scope of the license granted to the defendant.[168] They were not merely covenants and these features of the license were found to be violated by the defendants. By violating the license terms, the defendants exceeded the scope of the license; their conduct gave rise to an action for copyright infringement rather than merely for breach of contract.[169] While this opinion is encouraging for supporters of the open source movement, in-house counsel should pay close attention since it appears that violators of open source licenses could be exposed to copyright infringement liability.

---

[166] Stern & Kane, *supra* note 1, at 46.

[167] *Jacobsen*, 609 F. Supp.2d at 932.

[168] *Id*.

[169] *Id.* at 933.

In 2007 and 2008, the Software Freedom Law Center (SFLC) initiated lawsuits on behalf of Erik Andersen and Rob Landley, the principal developers of BusyBox.[170] The SFLC is the pro bono branch of Stallman's Free Software Foundation. [171] These lawsuits claimed that Verizon, Monsoon Multimedia, High-Gain Antennas and Xterasys, Super Micro Computer, Inc., and Extreme Networks, Inc. violated version 2 of the GNU General Public License (GPLv2). The grounds for the claims were alleged distribution by the defendants of products that contained BusyBox code. The critical factor was that these products were released without the underlying source code, thereby breaching the terms of the GPLv2.[172] As of October 2008, only Extreme Networks action remained outstanding.[173] Generally the settled actions contained two similar components in their resulting agreements. First, the defendants agreed to appoint an internal Open Source Compliance Officer who would function to monitor compliance with GPL licenses, and to publish the source code for the version of BusyBox they previously distributed.[174] The second element of the settlements involved undisclosed payment by defendants to BusyBox's developers.[175]

There are important points to take away from the recent settlements and litigation. The redistribution of software under hereditary licenses is complex. It can easily frustrate even a

---

[170] The complaints were all filed by the Software Freedom Law Center, Inc. For the complaint against Monsoon Multimedia, Inc., *i.e.*, the first suit filed, see *Anderson v. Monsoon Multimedia, Inc*. Complaint No. 07-cv-08205-JES (S.D.N.Y. Sept. 19, 2007), *available at* http://www.softwarefreedom.org/news/2007/sep/20/busybox/complaint.pdf.

[171] Stern & Kane, *supra* note 1, at 45.

[172] *See* source cited supra 170, at 5.

[173] Stern & Kane, *supra* note 1, at 45.

[174] *Id.*

[175] *Id.*

savvy, sophisticated company's ability to manage its exposure to risk. Consequently, focus on internal compliance is extremely important. Companies using open source code cannot rely on the ill-conceived notion that open source licensing is irrelevant to their line of work.[176]

Moreover, the SFLC created Moglen Ravicher LLC, a firm employing the very lawyers who instituted the original five suits discussed above, to represent for-profit clients in GPL license violation claims.[177] It is foreseeable that, going forward, more firms will undertake this type of litigation on a contingency fee basis.[178] Actions regarding open source licensing enforceability are not limited to the United States.[179] In 2007, Harald Welte brought a series of German enforcement actions for alleged violations of the GPLv2.[180] Welte was in the business of running the gpl-violations.org project. The court found in his favor in one such suit against Skype Technologies SA.[181]

Open source software invites a plethora of legal interpretations and applications based just on the few actions that have been litigated.[182] For example, courts have been faced with the question of determining whether a license agreement was created.[183] Typically programmers using open source code do not sign a license agreement and the threshold issue in some actions is

---

[176] Stern & Kane, *supra* note 1, at 46.

[177] *Id.*

[178] *Id.*

[179] *See generally* Harald Welte's Blog, http://laforge.gnumonks.org/weblog/linux/gpl-violations/.

[180] *Id.*

[181] *Id.*

[182] Stern & Kane, *supra* note 1, at 46.

[183] *Id.*

degree of enforceability of "browsewrap" agreements.[184] The Free Software Foundation and other attorneys have taken the view that open source licenses are not contracts.[185]

Another area of dispute centers around whether the nature of open source software creates infringement issues where there are existing patents. Microsoft has publicly alleged that the Linux operating system (which competes against Microsoft's Windows) violates a large number of Microsoft's patents and that other open source code infringes upon over 200 Microsoft patents.[186] Despite the various interpretations of legal issues surrounding open source code, the risks associated with its use in commercial settings remain high as a result of the lack of guidance from the courts in this developing area.

CONCLUSION

Despite its risks, open source carries with it many benefits. It can be a cost-effective alternative to purchasing software. The communal contributions and collaboration of ideas that sculpt and create the derivative, modified or redistributed works bring highly positive synergistic results that cannot be denied. With the right group of informed professionals, open source can be managed effectively.[187] Open source code and the associated licenses may seem daunting at first, particularly to lawyers accustomed to having a tangible, signed paper agreement before use

---

[184] LORI LESSER, *Open Source Software 2006: Critical Issues in Today's Corporate Environment*, Practising Law Institute: Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 885 PLI/Pat 9, 26 (2006).

[185] *See* Matt Lee, *What is Free Software and Why is it so Important for Society?*, FREE SOFTWARE FOUNDATION, March 29, 2010, http://www.fsf.org/about/what-is-free-software.

[186] Roger Parloff, *Microsoft Takes On The Free World*, FORTUNE, May 14, 2007, http://money.cnn.com/magazines/fortune/fortune_archive/2007/05/28/100033867/. Microsoft has also entered into a number of "cross-licensing agreements," which may really be cross-covenants not to sue with open source software companies regarding IBM's patents.

[187] Stern & Kane, *supra* note 1, at 49.

of the software can begin; however, open source code can be manageable with the cooperation of software development teams and other legal and compliance professionals.

Attorneys have a vested interest in broadening their horizons of knowledge on open source software. The omnipresence of the software makes it critical to the legal profession, particularly for general counsel and even more critical for in-house counsel to technology and engineering firms. Awareness, understanding and a basic plan for due diligence is crucial for lawyers who will absolutely be faced with the ramifications of the GPLv3 on proprietary intellectual property assets. With pro-activity and open-communication channels between upper management, legal counsel and engineers, open source can be managed effectively and safely. The ease and benefits of its use have contributed to its prevalence, requiring the attention of internal counsel, corporate attorneys and intellectual property attorneys.

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 5, PAGE 112

The Future Control of Food: A Guide to International Negotiations and Rules on Intellectual Property, Biodiversity and Food Security

Edited by Geoff Tansey and Tasmin Rajotte

Citation: THE FUTURE CONTROL OF FOOD: A GUIDE TO INTERNATIONAL NEGOTIATIONS AND RULES ON INTELLECTUAL PROPERTY, BIODIVERSITY AND FOOD SECURITY (Geoff Tansey & Tasmin Rajotte eds., Earthscan Publications Ltd., 2008).

Reviewed by: Caitlyn Whitehead*

Relevant Legal and Academic Areas: Intellectual Property, Patents, Food and Drug Law, Biotechnology.

Summary: The collection provides an overview of international agreements regarding biodiversity and food security. It is divided into 3 parts, each part containing entries and chapters written by different authors and experts in the area, including law professors, attorneys, consultants, and policy makers. Part I of the book offers an introduction to intellectual property law, the global food system, and the role and importance of laws and regulations of the system on a national and worldwide scale. Part II gives a background on negotiations in this area, as well as more detailed information on the key negotiations and agreements in the global system today, including: The Agreement on Trade-Related Aspects of Intellectual Property Rights, The International Treaty on Plant Genetic Resources for Food and Agriculture, and the World Intellectual Property Organization. This section also addresses the inconsistencies among the various programs and agreements and the main questions that arise in the control of genetic resources. Part III contains some reactions to the impact of these changing rules and regulations on research and development and the impact of the negotiations on society and the economy. It goes further to draw conclusions about the negotiating process, alternatives, and needed innovations.

About the Editors: Geoff Tansey is a researcher and writer on food, agriculture and intellectual property. From their inception to 2007, he has been the senior consultant for the intellectual property and development programs of the Quaker United Nations Office in Geneva and the Quaker International Affairs Program in Ottawa. He is also a director of the Food Ethics Council. Tasmin Rajotte has a master's degree in environmental science, and is the Quaker Representative for the Quaker International Affairs Programme in Ottawa.

* J.D. candidate, Syracuse University College of Law, expected 2010; Associate Editor, *Syracuse Science & Technology Law Reporter*.

Part I: A Changing Food System

Chapter 1: Food Farming and Global Rules, *Geoff Tansey*

- **Chapter Summary:** This chapter provides an overview of what Tansey calls the current "dominant food system."[1] The chapter provides a background of intellectual property and the increasing role of intellectual property in food and farming. It also addresses the concerns prompted by this growing system.

- **Chapter Discussion:** The chapter begins by introducing the various institutions that play key roles in the regulation of food and farming, focusing on the importance of the creation of the World Trade Organization (WTO) in 1995. The creation of this organization was so important because it brought agriculture fully under the trade regime for the first time.[2] Since intellectual property rights were included in the WTO agreement, this meant that all aspects of agriculture were now subject to IP regulation, which was opposed by, and dramatically effects, developing countries.[3] One reason for this opposition is that, due to the nature of negotiations, it is relatively difficult for smaller and lower-income countries to influence the outcome of the negotiations.[4]

Next, Tansey discusses the food system itself. Due to the nature of the subject, food policy enactment is inherently difficult and complex. An essential element of this is biodiversity and environmental stability, without which the global food supply will suffer.[5]

---

[1] THE FUTURE CONTROL OF FOOD: A GUIDE TO INTERNATIONAL NEGOTIATIONS AND RULES ON INTELLECTUAL PROPERTY, BIODIVERSITY AND FOOD SECURITY (Geoff Tansey & Tasmin Rajotte eds., Earthscan Publications Ltd., 2008) [hereinafter Tansey & Rajotte].

[2] *Id*. at 6.

[3] *Id*. at 7.

[4] *Id*.

[5] *Id.* at 7-8.

The global food system, according to Tansey, is characterized by a struggle between power and control over production and food , and who will reap the benefits and bear the risks arising thereof.[6] He views three key trends as having affected the development of the food system.[7] The first is the growing concentration of power so that fewer firms control more of the market.[8] The concentration of power allows those who benefit from the concentration to control price, standards, and competition.[9] The second is the shift from local markets to larger markets, and the third are the tools that alleviate the risks to certain actors in the market.[10]

The first such tool is science and technology. The second is information management. By this, Tansey means that the spread of information, especially through various media outlets, affects food habits by globalizing products and reinforcing brand images.[11] The next tool is the law, specifically intellectual property. Tansey beings with a basic definition of intellectual property: "legal and institutional devices to protect creations of the mind such as inventions, works of art and literature, and designs."[12]

Tansey first discusses the origins of intellectual property protections, and then goes on to address various concerns. One of these concerns is regarding the effects of intellectual property on access to knowledge and goods, the effects on research and development, and concentration

---

[6] Tansey & Rajotte, *supra* note 1, at 8.

[7] *Id.*

[8] *Id*.

[9] *Id*.

[10] *Id*. at 9-10.

[11] Tansey & Rajotte, *supra* note 1, at 10.

[12] *Id.* at 12.

of power.[13] Another concern is whether the intellectual property regime adequately balances competing interests.[14]

There are arguments for and against having intellectual property. Tansey explains that proponents assert that it is necessary to provide reward, security, and incentive for innovation.[15] The utilitarian approach recognizes that to invest time and other resources into innovation, there needs to be an incentive. Giving IP rights, through a patent for example, gives the creator the incentive, and enhances market power of the product.[16] An argument against is that greater IP rights may actually lead to less innovation. He cites Peter Drahos' idea that instead of viewing them as proprietary rights, we should view them as privileges.[17] The major problem, says Tansey is whether the system really establishes equality. This leads to his discussion of patents.

In the United States, patents are granted for the invention of something new, useful, and no-obvious, and in Europe for having industrial application, novelty, and an inventive step.[18] However, Tansey asserts that patents are widely given for products that are not novel, or involving an "inventive step." He quotes Professor Stuart Macdonald of Sheffield University, who states that there is inequality in the system because those who are poor lack the money to enforce their patents.[19] He also sees a problem in the practice of the patent system: when

---

[13] Tansey & Rajotte, *supra* note 1, at 12.

[14] *Id*.

[15] *Id*. at 15.

[16] *Id*.

[17] *Id.* at 16.

[18] Tansey & Rajotte, *supra* note 1, at 17.

[19] *Id*.

following the guidelines the inventor rarely has to actually give enough information for the public to replicate the invention.[20]

Tansey ends the chapter with a discussion of the role of intellectual property in food and farming. A major facet of this is advertising and trademarks for certain product brands.[21] This creates a discrepancy between those producers who can afford global marketing and those who cannot.[22] Producers, however, are still limited by the rights of others if, as in the example of crops, the plant breeder holds intellectual property rights in the seed used to produce the particular plant variety.[23]

Part II: The Key Global Negotiations and Agreements

Chapter 2: Turning Plant Varieties into Intellectual Property: The UPOV Convention, *Graham Dutfield*

- **Chapter Summary:** In this article, Graham Dutfield addresses the political nature of intellectual property law. The chapter also looks at the development of plant breeder's rights and discusses the nature and problems of plant variety protection (PVP) and the International Union for the Protection of New Varieties of Plants (UPOV).

- **Chapter Discussion:** Dutfield starts his introduction to breeder's rights with a background and history of the science of plant breeding. The process is characterized by the separation between farming and breeding, which Dutfield says is still occurring in some areas, or

[20] Tansey & Rajotte, *supra* note 1, at 17.

[21] *Id*. at 19-20.

[22] *Id.* at 20.

[23] *Id.*

has not even begun.[24] This change began in the early 19th century, when breeders began to separate themselves in the market and increased application of genetics to the practice.[25] Generally, the process involves crossing two or more plant varieties with desirable traits to produce new varieties. Other techniques include hybridization and the development of tissues and cell cultures.[26]

The modern seed industry emerged as a result of these new techniques. The industry went from rather experimental, with the Patent Office and the USDA providing farmers with free experimental seed packets, to public and private sector programs.[27] An important landmark occurrence in the rise of the private seed industry was the breeding of hybrid corn.[28]

The UPOV Convention established the UPOV, which enacted the plant variety protection (or plant breeder's rights) regime.[29] The provisions of the Convention state which varieties are covered, the requirements for protection, the length and scope of protection, and various exemptions and privileges.[30] To be covered, a variety must be new, distinct, stable and uniform.[31] The original UPOV in 1978 defines the scope of rights as "the production for purposes of commercial marketing; the offering for sale; and the marketing of the reproductive

---

[24] Tansey & Rajotte, *supra* note 1, at 27.

[25] *Id.* at 27-28.

[26] *Id*. at 28.

[27] *Id.* at 30.

[28] *Id*.

[29] Tansey & Rajotte, *supra* note 1, at 32.

[30] *Id.* at 34.

[31] *Id*. at 35.

or vegetative propagating material, as such, of the variety."[32] In 1991, this was extended to include more protection for breeders by including more actions as requiring breeder authorization.[33] The convention requires breeder authorization for three acts: production for the purpose of commercial marketing, offering for sale, and the marketing of the reproductive material of the variety.[34] However, there is an exception for farmers, who may use saved seeds on the same farm.[35] The PVP protection lasts for a minimum of twenty years.[36]

Patents differ from PVP in a number of ways. Dutfield next discusses these differences between patents and PVP and why many breeders prefer PVP over the patent system. While patents provide greater legal protection, PVPs contain breeder's exemptions that allow breeders to access a greater variety of plant genetic material, which is most likely the reason for this preference.[37] While PVP was designed to coexist peacefully alongside patents, the two are often in tension with one another.[38]

One of the main concerns surrounding the UPOV is the suitability of the system for developing countries. Sub-issues of this are research priorities, the impact on small farmers, and the availability of genetic resources. The UPOV takes away the freedom of farmers to buy from

[32] Tansey & Rajotte, *supra* note 1, at 37.

[33] *Id* at 38-39.

[34] *Id* at 39.

[35] *Id.*

[36] *Id*. at 39.

[37] Tansey & Rajotte, *supra* note 1, at 40.

[38] *Id*. at 38.

those other than the original breeders of their varieties.[39] In addition to PVP, various seed laws play a role in these concerns.[40]

Chapter 3: Bringing Minimum Global Intellectual Property Standards into Agriculture: The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), *Pedro Roffe*

- **Chapter Summary:** This chapter looks at the history and impact of TRIPS (The Agreement on Trade-Related Aspects of Intellectual Property Rights). It also examines how TRIPS affects food security and surrounding issues.

- **Chapter Discussion:** TRIPS provisions are organized into seven parts: general provisions and basic principles, availability, scope and use of IPRs, enforcement, acquisition and maintenance of rights, dispute management, transitional agreements, and institutional arrangements.[41] TRIPS set up minimum standards of protection, and provided more comprehensive coverage then previous intellectual property regulations, and included enforcement.[42] The agreement also fully incorporated IP into the international trade system.[43] Another general provision of the agreement is non-discriminatory treatment among foreign bodies, and a national treatment principle which states that treatment of foreigners be "no less favorable" than the treatment afforded nationals.[44]

---

[39] Tansey & Rajotte, *supra* note 1, at 41.

[40] *Id.* at 42.

[41] *Id*. at 51.

[42] *Id.* at 53.

[43] *Id*.

[44] Tansey & Rajotte, *supra* note 1, at 53.

As to scope and duration, TRIPS provides that patents be available without discrimination related to where it was produced, the field of technology, and whether local or imported.[45] The only products that may be so excluded are those that offend public morality. It also addresses whether animals and plant organisms are patentable. It states that "members may exclude from patentability plants and animals other than micro-organisms, and essentially biological processes for the production of plants or animals other than non-biological and microbiological processes."[46] The members must, however, make patents for plant varieties available. This is controversial because it obligates members to provide patents for specific things. TRIPS also provides increased exclusivity of breeder's rights, including the right to prevent third parties not having owner's consent from making, using, selling, or importing the product for those purposes.[47] It also provides for compulsory licensing in certain situations, and procedure for civil patent infringement cases.[48] Roffe addresses the arguments for and against patent protection for plants and animals. Some of the arguments for are that it facilitates the transfer of technology and knowledge and that they should be afforded the same rights as other innovation.[49] Some arguments against are the cost and access implications of the patents.[50]

Roffe then describes the relationship between TRIPS and global food security. Members of TRIPS are authorized under the agreement to adopt measures that take into account nutrition

---

[45] Tansey & Rajotte, *supra* note 1, at 54-55.

[46] *Id*. at 55.

[47] *Id.* at 55, 57.

[48] *Id*. at 57.

[49] *Id*. at 63.

[50] Tansey & Rajotte, *supra* note 1, at 63.

and health consequences (so long as the measures are consistent with the agreement).[51] The relationship between TRIPS and the Convention on Biological Diversity (CBD) is also examined. A main concern is that TRIPS does not require compliance with important CBD provisions. For example, developing countries are concerned that TRIPS impinges on CBD's protection of traditional knowledge and folklore.[52]

Roffe addresses arguments that have taken place in the TRIPS council for and against international rules protecting traditional knowledge. Some of the arguments for protection are that traditional knowledge is a valuable global resource, protecting the culture of traditional communities, and the promotion of sustainable biodiversity.[53]

Chapter 4: Promoting and Extending the Reach of Intellectual Property: The World Intellectual Property Organization (WIPO), *Maria Julia Olivia*

- **Chapter Summary:** This chapter looks at the background and actions of the World Intellectual Property Organization and its impact on, and relationship with, intellectual property, food security, and biodiversity.

- **Chapter Discussion:** The WIPO has 183 member states, and was started in 1970, replacing previous organizations. It performs various tasks relating to the protection of intellectual property rights. Its convention states that the objectives of the organization are to: "promote the protection of intellectual property throughout the world…and to ensure administrative operations among the unions administered thereby."[54] Olivia describes the WIPO

[51] Tansey & Rajotte, *supra* note 1, at 59.

[52] *Id.* at 66.

[53] *Id*.

[54] *Id.* at 72.

as having the view of intellectual property as a "power tool" for development.[55] She states, that WIPO has been criticized for not viewing IP as a means of effectuating public policy.[56] As Olivia points out, intellectual property rights are created by national law and are, therefore, effective in those nations alone; but international agreements will often set minimum standards of protection.[57]

The WIPO is divided into several committees. Three of these are the Standing Committee on the Law of Patents (SCP), the Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore (IGC), and the Provisional Committee on Proposals Related to the WIPO Development Agenda (PCDA). The SCP focuses on patent law. The IGC focuses on the relation among intellectual property, genetic resources, traditional knowledge, and folklore, and the PCDA seeks to ensure that the organization takes into account the development concerns. One of the governing bodies of the WIPO, the General Assembly, discusses proposed rules and is responsible for much of the decision making.

Chapter 5: Safeguarding Biodiversity: The Convention on Biological Diversity (CBD),
Susan Bragdon, Kathryn Garforth and John E. Haapala Jr.

- **Chapter Summary:** This chapter discusses the Convention on Biological Diversity. It examines the origins of the convention and its relation to genetic resources, traditional knowledge, and the implementation and enforcement of the convention. A specific subsidiary of the CBD is discussed in depth, the Cartagena Protocol on Biosafety.

[55] Tansey & Rajotte, *supra* note 1, at 71.

[56] *Id*.

[57] *Id*.

- **Chapter Discussion:** There are three major sources from which the CBD originated, which are described in this chapter. One was concern over whether international agreements adequately addressed all of the issues, areas and species in the protection of wildlife.[58] The second is the move toward sustainability in conservation policy, and the third are issues of access.[59]

The CBD itself, which is concerned with biological diversity, has three objectives: the conservation of biological diversity, its sustainable use, and the "fair and equitable sharing of the benefits arising out of utilization of genetic resources…"[60] The authors focus on five areas of the convention in their discussion. The first is access to genetic resources and benefit sharing.[61] This is addressed in article 15 of the Convention. Generally, the article calls for the treatment of genetic resources as national resources, subject to national legislation. It also furthers the Convention's aim of sovereignty over resources.[62] The issue of access to resources is central to this section.

The second area is traditional knowledge. Article 8(j) provides that the national legislation to: "respect, preserve and maintain knowledge, innovations and practices of indigenous and local communities embodying traditional lifestyles relevant for the conservation and sustainable use of biological diversity, promote their wider application with the approval and involvement of the holders of such knowledge, innovations and practices, and encourage the

---

[58] Tansey & Rajotte, *supra* note 1, at 84.

[59] *Id.*

[60] *Id*. at 85.

[61] *Id*. at 86.

[62] *Id.*

equitable sharing of the benefits arising from the utilization of such knowledge, innovations and practices."[63]

The third and fourth areas of the Convention addressed are that of innovations and the transfer of technology. This is found in Article 16. As the authors point out, this is the only explicit reference to intellectual property in the Convention.[64] In this section, the Convention states that access of developing countries to, and transfer of technology shall be provided for and facilitated.[65] Further, it calls for the facilitation of access to and transfer of technology from the private sector to government institutions and developing countries.[66] It also states that parties shall cooperate concerning intellectual property rights for effective transfer and use among the parties. The fifth and final area is the implementation, compliance and enforcement of the Convention.

Following the discussion on the Convention, the authors go into further detail regarding a subsidiary of the Convention, the Cartagena Protocol on Biosafety. The protocol focuses on reducing the potential risks from modern biotechnology (specifically from living modified organisms, or LMOs).[67] LMOs are defined in the protocol as "any living organism that possesses a novel combination of genetic material obtained through the use of modern

---

[63] Tansey & Rajotte, *supra* note 1, at 91.

[64] *Id*. at 92.

[65] *Id*.

[66] *Id*. at 94.

[67] *Id.* at 106.

biotechnology."[68] One key issue in the protocol is the labeling of shipments and documentation required of shipments of LMOs.[69]

Chapter 6: Giving Priority to the Commons: The International Treaty on Plant Genetic Resources for Food and Agriculture (ITPGRFA), *Michael Halewood and Kent Nnadozie*

- **Chapter Summary:** This chapter discusses the Treaty and the negotiations that led to its development and adoption.

- **Chapter Discussion:** The Treaty's main aim is the conservation and sustainability of plant genetic resources for food and agriculture (PGRFA). The author says that human activity is the driving force behind agricultural biodiversity.[70] Those who developed the Treaty believed that agricultural biodiversity should be treated differently in access and benefit sharing than others in the CBD.[71] The Treaty creates a commons, where access to plant genetic resources for various uses is freely available among parties to it. Regulation of PGRFAs was needed, the authors state, because of the distinct nature of the resources.[72] To operate the commons, the Standard Multilateral Trade Agreement was also entered into, to govern the transfer of materials in the new multilateral system.[73] The Treaty also includes provisions for farmers' rights, access and benefit sharing, support, and financial and institutional issues.

---

[68] Tansey & Rajotte, *supra* note 1, at 106.

[69] *Id.* at 108.

[70] *Id*. at 115.

[71] *Id.*

[72] *Id*. at 116.

[73] Tansey & Rajotte, *supra* note 1, at 116.

Chapter 7: The Negotiations Web: Complex Connections, *Tasmin Rajotte*

- **Chapter Summary:** This chapter discusses the complexity of a system which contains many international treaties, negotiations, and agreements, which sometimes are in conflict with one another. There are several strategies for harmonization that Rajotte proposes. Some of these strategies are forum management and bilateral and regional trade agreement, enforcement mechanisms, WTO accessions, and the implications for genetic resources.

- **Chapter Discussion:** The first strategy discussed is forum management and bilateral and regional trade agreement. Larger, more powerful countries engage in what Rajotte calls "forum shopping": when they cannot get the level of protection they want from one forum, they shift to another.[74] Rajotte also describes a number of provisions of bilateral and regional free trade agreements (FTAs) that are focused on agriculture. Many FTAs have requirements that signatories also become parties to the UPOV to protect plant breeder's rights.[75] Others include requirements to introduce patent protection for plants, animals, and biotechnological inventions.[76] The United States has started to introduce contract terms into its agreements.[77] As to enforcement, free trade agreements will usually specify how disputes will be handled.

As to WTO accessions, all members of the WTO are also party to TRIPS, which is the one multilateral trade agreement for which this is the case. Some countries are imposing greater accessions, such as UPOV ratification. Biopiracy is defined by the authors as corporations from industrialized countries taking the genetic resources, traditional knowledge, and technologies of

[74] Tansey & Rajotte, *supra* note 1, at 142.

[75] *Id.*

[76] *Id*.

[77] *Id*. at 143.

developing countries, and includes the following actions: the unauthorized use of common traditional knowledge, the unauthorized use of TK only found among one indigenous group; the unauthorized use of TK acquired by deception or failure to fully disclosure the commercial motive behind the acquisition; the unauthorized use of TK acquired on the basis of a transaction deemed to be exploitative; the unauthorized use of TK acquired on the basis of a conviction that all such transactions are inherently exploitative; and the commercial use of TK on the basis of a literature search.[78] Related to patents, such actions include the patent claims TK in the form in which it was acquired; the patent covers a refinement of the TK; and the patent covers an invention based on TK *and* other modern/traditional knowledge.[79]

Shaping relationships between international agreements is complicated. Some claim that the CBD and TRIPS work together, while others believe that they are somewhat inconsistent. Generally, industrialized nations see no conflict, while some developing nations hope to reconcile the two, through a revision of TRIPS.[80] The chapter also discusses the relationship and conflict of these with ITPGRFA and the UPOV. The difference between WIPO and other international instruments is also discussed. To facilitate the implementation of TRIPS, an agreement on cooperation between WTO and WIPO was entered in 1995, for example, which provides for cooperation in certain areas, including notification, implementation, and technical cooperation.[81]

---

[78] Tansey & Rajotte, *supra* note 1, at 147-48.

[79] *Id.* at 148.

[80] *Id*. at 150.

[81] *Id*. at 156.

The chapter closes by discussing the implications of the conflicts between instruments on genetic resources food and agriculture. Conflict between countries may arise over sources of origin and sovereign rights. Another issue is the risk of conflict between human rights law and trade law and policy, with trade law and policy affecting developing nations' access significantly.

Part III: Responses, Observations and Prospects

Chapter 8: Responding to Change, *Heike Baumüller and Geoff Tansey*

- **Chapter Summary:** This chapter addresses some of the responses to the rules discussed and the concerns regarding them.

- **Chapter Discussion:** One criticism of intellectual property is that it places too much restriction on access and use.[82] The concern is that the IP system has implications on global food security. Another criticism is the concentration of power in powerful corporate entities within industrialized nations.[83] New agreements, the authors say, have also failed to adequately address the complex issues arising from traditional knowledge and folklore according to some developing nations.[84] The major responses focus on issues of access and implementation of technology transfer and genetic resource sharing.

Much concern has been focused on patents. The rules governing these patents have been said to focus more on private interests than the interests of the public. One response to this was the IPR commissions' recommendation that developing countries do not allow plants and

[82] Tansey & Rajotte, *supra* note 1, at 174.

[83] *Id.* at 175.

[84] *Id*. at 178.

animals to be subject to patent, develop different forms of plant variety protection, strengthen public research, and ratify the ITPGRFA and its farmers' rights provisions.[85] Another concern in this area is that traditional knowledge is being used at a disadvantage to developing countries where such knowledge originated.

Chapter 9: Postcards from International Negotiations, *Peter Drahos and Geoff Tansey*

- **Chapter Summary:** This chapter looks back at the discussion of the previous chapter and makes observations on the various international agreements and instruments. It addresses some of the issues arising from biodiversity, food security, and intellectual property.
- **Chapter Discussion:** The authors approach this chapter by discussing various leverage points. The first of these is structural leverage. Structural leverage is institutionalized economic and military power.[86] Larger more powerful countries have more of this type of leverage.

The second the authors call floating points of leverage. The authors use the example of Ethiopia—while it does not have much structural leverage, it was able to become a key negotiator over the Cartagena Protocol on Biosafety because of floating points of leverage, such as technical capacity and the building of relationships and networks.[87] The third is choosing multilateral over bilateral agreements. The authors assert that multilateral fora are better for the less powerful actors in the system than bilateral because such agreements provide more opportunities for leverage for these countries.[88] Another suggestion made by the authors is to

[85] Tansey & Rajotte, *supra* note 1, at 182.

[86] *Id.* at 200.

[87] *Id*. at 201.

[88] *Id.* at 202-03.

solve issues of biodiversity with scientific and evidence based negotiation rather than legal based negotiation.[89]

Chapter 10: Global Rules, Local Needs, *Geoff Tansey*

- **Chapter Summary:** This chapter is a conclusion to the former, and looks to the future and the role of the rules discussed in influencing various outcomes.

- **Chapter Discussion:** The current rules will affect future food systems. Tansey suggests that they "will encourage or discourage different kinds of roles of small farmers, different approaches to biodiversity, and different approaches to the distribution of wealth and power."[90] One issue is that there is a lack of incentive for conservation and use of biodiversity by farmers, but more of a focus on commercial interests.[91] He predicts that as the impact of global rules on intellectual property, biodiversity and agriculture become more apparent, the public debate will shift toward the importance of these, and many of these conflicts will likely need to be addressed and resolved.[92]

[89] Tansey & Rajotte, *supra* note 1, at 208.

[90] *Id.* at 214.

[91] *Id*. at 216.

[92] *Id*. at 219.

SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 6, PAGE 131

Patent Failure: How Judges, Bureaucrats, and Lawyers Put Innovators At Risk

By: James Bessen & Michael J. Meurer

Citation: JAMES BESSEN & MICHAEL J. MEURER, PATENT FAILURE: HOW JUDGES, BUREAUCRATS, AND LAWYERS PUT INNOVATORS AT RISK 2 (Princeton University Press, 2008).

Reviewed by: Susan C. Azzarelli*

Relevant Legal and Academic Areas: Patents; Property Rights; Economics; Legal Reform

Summary: *Patent Failure* takes a comprehensive look at the economic performance of patents over the last 40 years in order to determine if the patent system is fundamentally broken, or if it can be repaired with modest reforms. The book's findings provide evidence from history, law and economics that patents provide incentive to invest in research and development, but fail to provide predictable property rights. By illuminating the shortcomings of unpredictable legal boundaries, *Patent Failure* calls for a change in laws and presents reform proposals.

About the Authors: James Bessen is a former software developer, who now is a lecturer at Boston University School of Law. He is an editor of *Technological Innovation and Intellectual Property*, and his work and research on patents and economics have been published in many journals.[1] Bessen also founded and is the director for Research on Innovation, a nonprofit organization which sponsors and promotes research on technological innovation.[2]

Michael J. Meurer is the Micheals Faculty Research Scholar and a professor of law at Boston University, where his courses include patents, intellectual property and public policy toward the high-tech industry. He was an expert witness for the Federal Trade Commission concerning issues of patent licensing. Meurer has also taught American intellectual property law at universities in Singapore and Canada.[3]

---

* J.D. candidate, Syracuse University College of Law, expected 2010; Executive Editor, *Syracuse Science & Technology Law Reporter*.

[1] About James Bessen, http://www.bu.edu/law/faculty/profiles/fullcvs/part-time/bessen_j.html.

[2] Research on Innovation, http://www.researchoninnovation.org/about.htm.

[3] About Michael J. Meurer, http://www.bu.edu/law/faculty/profiles/bios/full0time/meurer_m.html.

Chapter One: The Argument in Brief

- **Summary**: Even with law, property systems can fail without supportive institutions and technical details that make sense and provide clear boundaries. When patents work correctly they should reward innovators and encourage investment in innovation. However, there has been failure of property right because patent related institutions and patent law have failed to get the details right.[4]

- **Discussion**: "Patents do not provide an affirmative right to use an invention… patents provide partial rights to exclude others from using an invention."[5] Because of failures in the American patent system the incentive to innovate is not always present. Property rights can fail when their validity is uncertain, when rights are so fragmented that the cost to negotiate makes the investment prohibitive, when boundary information is not publically accessible, and when the boundary rights are not clear and predictable.[6]

The important difference between the implementation of property rights and that of patent rights is the notice function, which does not always function as well within the patent system. Poor notice can cause harm because there are unavoidable risks for dispute and litigation because of inadvertent infringement, which creates a disincentive for innovation.[7] The institutional features of patent notice often include fuzzy and unpredictable boundaries, an inability for the public to access patents because they can be kept hidden for years, issues with possession and the scope of rights because an inventor may not actually have possession and an

[4] JAMES BESSEN & MICHAEL J. MEURER, PATENT FAILURE: HOW JUDGES, BUREAUCRATS, AND LAWYERS PUT INNOVATORS AT RISK 2 (Princeton University Press, 2008).

[5] *Id*. at 6.

[6] *Id*. at 7.

[7] *Id.* at 9.

increased clearance cost because of the need to check prospective rights for infringement.[8] A better system would provide defined and exclusive rights.

"Patents do not work 'just like property'".[9] While patents provide some rights for their owners, the potential effect on others' patents includes a high risk of litigation and increased cost as the frequency of litigation continues to grow. Difficulties with notice are consistent with litigation costs. Litigation cost is low for the pharmaceutical industry, which patents chemical compounds with clear boundaries, but high for software patents where boundaries are not easily determined.[10] Patents will benefit from better notice standards, and it may help them function more like property.

Chapter Two: Why Property Rights Work, How Property Rights Fail

- **Summary**: Although most people understand patents to be a type of property, scholars are not comfortable with the label.[11] Patent law differs from property law in that it only grants negative rights to exclude but does not give the affirmative right to use and invention.[12] Although trespassers on tangible property or on patent rights are liable for the infringement regardless of their intent, neither right is absolute.

- **Discussion**: Tangible property owners can sell, divide and rent their property. Similarity patent owners can do the same, but the rental to licensing parallel is not exact because a patent

[8] BESSEN & MEURER, *supra* note 4, at 10.

[9] *Id.* at 14.

[10] *Id.* at 18.

[11] *Id.* at 29.

[12] *Id.* at 30.

owner can license to many people without degrading the value of the information.[13] Although patents share some key features of the tangible property system, there are prominent differences. "Patent law offers weaker rights that property law along four dimensions… patents in the United States are limited to twenty years…there is no affirmative right to use…it only extends to inventions that are new, useful, non-obvious, and of the proper subject matter… and patent damages do not include a defendants profit."[14] Patent law does allow more freedom in the design of contracts and supports a variety of indirect forms of liability that allow the patent owner to bring suit,[15] however not all inventions are patentable.

The property system does not always work, and "severe uncertainty about ownership, the scope of rights, and the effectiveness of the courts causes significant deterioration in the performance of property."[16] Uncertainty creates impediments to efficient use and investment. "The effectiveness of property rights is sensitive to the details of implementation. The benefits of private property derive from the promise of efficient, non-arbitrary enforcement."[17] The disputes and litigation plaguing the patent system stem from poor implementation.

Chapter Three: If You Can't Tell the Boundaries, Then It Ain't Property

- **Summary**: "A successful property system establishes clear, easily determined rights."[18] Clarity leads to efficiency because strangers to a property can avoid trespass and other rights

[13] BESSEN & MEURER, *supra* note 4, at 31.

[14] *Id.* at 33.

[15] *Id.*

[16] *Id.* at 39.

[17] *Id.* at 45.

[18] BESSEN & MEURER, *supra* note 4, at 46.

violations, or negotiate use of the property. "Patents fail to provide *clear notice* of the scope of patent rights."[19] Because it has become increasingly difficult to determine whether the technology infringes on another's patent rights, there is a significant problem with inadvertent infringement in the patent system. "Property law provides good notice to potential purchasers about the property rights relevant to a contemplated land use," and "has stable doctrine and flourishing institutions designed to transmit clear notice."[20] Patent law lacks such components.

- **Discussion**: There are four aspects to the notice problem: inventors can hide patent claims and thus boundary information, even with public access patent claims are difficult to interpret, there is a danger that the meaning of the language in the claim will change, and even when the claims are available over a clear fixed time the cost to search them is quite high.[21] These aspects reinforce each other and make inadvertent infringement more likely.

Designing around patents can be difficult and expensive. Disputes over patent rights often occur because infringers were unaware of the earlier invention and the patent rights, or because the set of potentially relevant patents have a large scope of vague claims.[22] The authors use the example of disputes between Kodak and Polaroid. Kodak was the dominant firm in American photography and helped Polaroid introduce instant photography in the 1940s.[23] Kodak researched instant photography and took great care to invent around Polaroid's patents, but still lost the patent suit filed by Polaroid a week after they entered the market.

---

[19] BESSEN & MEURER, *supra* note 4, at 46.

[20] *Id.* at 54.

[21] *Id*. at 71.

[22] *Id.* at 47.

[23] *Id.* at 48.

"An innovator can even get a patent on his technology, and still be liable for infringement of someone else's patent."[24] There are many patents which may apply to new technologies because they are granted wide and uncertain scope making it difficult to determine validity. Even where validity may be determined, to do so accurately may be too expensive.[25] It is too difficult to determine boundaries of technology, and innovators cannot easily and reliably determine whether they are infringing on others' patent rights.

This also creates problems with the courts. Patent cases are heard in the Federal Circuit, which has been skeptical about including extrinsic evidence for claim construction because although it would strengthen notice, it would decrease the courts role and power.[26] The court currently applies the doctrine of equivalents, which was designed to protect inventors against the risk of pirates, and today applies with no regard to motive or methods of infringement, actually corroding the notice function of patents.[27] This can also affect possession rights, because broad claims allow patents on technology a person has not actually invented yet. Judges have not consistently limited ownership of technology actually possessed.[28]

Chapter Four: Survey of Empirical Research: Do Patents Perform Like Property?

- **Summary**: It is suggested that property based incentives explain the United States' technological leadership, but the connection between a nation's technology and the

[24] BESSEN & MEURER, *supra* note 4, at 49.

[25] *Id.* at 50-51.

[26] *Id.* at 61.

[27] *Id*.

[28] *Id.* at 68.

sophistication of its patent system is not enough of a link to explain the incentives.[29] The differences between patents and tangible property or financial property can affect the link between patents and economic growth.

- **Discussion**: Historically, Britain had well defined property rights, but patent litigation was costly, courts were not always sympathetic to patent holders, and patents could be invalidated.[30] The cost of litigation offset the gains from patents. Even with flaws, the U.S. patent system has had a more positive effect on innovation and economic growth than in Britain because of their ready availability and the economic growth that occurred from 'thickets' and patent pools which expanded market power.

Intellectual property rights may encourage research and development spending but the effect is too small to show major influence on economic growth.[31] At best, there is only a weak and indirect relationship to economic growth. "Effective economic performance depends on well-developed public and private institutions to support the property system and [those] are often more difficult to develop."[32] It was shown even in the pharmaceutical industry, where patents are generally beneficial, that strengthening patent coverage doesn't increase innovation.[33] The evidence shows that patents do not universally stimulate economic growth and innovation,

[29] BESSEN & MEURER, *supra* note 4, at 73-74.

[30] *Id.* at 78.

[31] *Id.* at 83.

[32] *Id.* at 85.

[33] *Id.* at 87.

nor do they stifle it. But, the positive effects of patents are highly contingent on the different industries and technology.[34]

Chapter Five: What Are U.S. Patents Worth to Their Owners?

- **Summary**: A poorly functioning property system imposes costs that arise from unanticipated disputes and litigation costs.[35] To determine the worth of patents the benefits as well as the costs from disputes must be considered.

- **Discussion**: Patents provide incentive through the rewards they provide, often in extra profits or 'rents'.[36] However, to get value from a patent the holder or firm must have market power. The value of patents can also be seen from patent renewals and what owners are willing to pay for them. Because technologies change over time, the value changes as well. If a patent owner declines a fee of $1,000, then it can be inferred that the patent is not worth $1,000 to the owner.[37]

Chemical patents are more valuable than other patents. "The boundaries that claim chemicals are more clearly defined than the boundaries of patents claiming complex technologies . . . that is chemical patents might provide stronger exclusion because they might be more likely to be successfully enforced."[38] The greater the likelihood that the patents will be successfully enforced, the greater the value to the holder.

---

[34] BESSEN & MEURER, *supra* note 4, at 92.

[35] *Id.* at 96.

[36] *Id.* at 97.

[37] *Id.* at 100.

[38] *Id.* at 107.

Research and development firms also look to means other than patents to get returns on their investment, since it is often the case that "the value of the patents might be far less than the value of the knowledge related to the associated inventions."[39] About 85 percent of an asset's value is not via patents and is not generally described as intellectual property.[40] Therefore, patents are not the only form of "rent" a firm may earn, and they may more likely come from licensing agreements. However, "certain groups of innovators do receive large rewards from patents, and patents might nonetheless provide an important incentive for some innovators."[41]

Chapter Six: The Cost of Disputes

- **Summary**: Because every dollar invested in research and development risks infringement, the cost of disputes reduces the profits innovators make on their investments and can reduce the incentive to invest.[42] Despite positive incentives in the pharmaceutical and chemical industries, the net incentive on other industries is generally negative. Patents put "a drag on innovation," slowing progress that could be much greater.[43] The value of patents has also not risen in value to meet the rise in lawsuits, legal costs and damages.[44]
- **Discussion**: The growing expense of lawsuits occurs because firms invest millions in research and development of technology that is owned by others.[45] Most lawsuits stem from

[39] BESSEN & MEURER, *supra* note 4, at 113.

[40] *Id.*

[41] *Id.* at 118.

[42] *Id.* at 120.

[43] *Id.* at 146.

[44] BESSEN & MEURER, *supra* note 4, at 146.

[45] *Id.* at 121.

inadvertent infringement and not from cheaters or copyists. "The more a firm spends on R&D, all else being equal, the *more* likely it is to be sued for infringement."[46]

Frequently patent holders claim a product is infringing once it is publically observable. This was the issue in the BlackBerry case in which RIM publicized its infringing technology, and NTP brought suit following the press release.[47] In that case, if RIM had been a cheater they would have been more likely to settle, instead of incurring the high legal fees of litigation and the business losses caused by the suit. "Patent litigation is uncertain…because the boundaries of patents are not clear and because the validity of litigated patents might be challenged."[48] The uncertainty leads to inadvertent infringement, because few are found to have intentionally cheated.

"Patent litigation is a real problem for innovators and its does impose a cost on investment in innovation."[49] Litigation costs can affect innovators in more than one way. They come both from the difficulty in enforcing patents and from infringing on someone else's patents.[50] Costs depend on how far the suit progresses but cases that make it to discovery can be quite costly, producing half the cost of cases that go to trial.[51] This is especially problematic because patent owners can sue anyone making, using, or selling a patented technology.[52]

---

[46] BESSEN & MEURER, *supra* note 4, at 124.

[47] *Id.*

[48] *Id.* at 125.

[49] *Id.* at 127.

[50] *Id.* at 131.

[51] BESSEN & MEURER, *supra* note 4, at 131.

[52] *Id.* at 133.

Predictable benefits are important to patents, and because the high cost of patent litigation is predictable "patents very likely provide a net *dis*incentive for innovation."[53]

Chapter Seven: How Important Is the Failure of Patent Notice?

- **Summary**: Patent notice failure and inadvertent infringement, as well as litigation stemming from such infringement, ultimately result in the failure of patents to provide positive innovation incentives.[54] The shortcomings of the patent system are the cause of increased litigation and the failure of patents to function as property. "[T]he deterioration of the notice function might be the central factor fueling the growth in patent litigation."[55]

- **Discussion**: During the 1990s, the use of continuing patent applications and the duration of patent prosecution provided more opportunity for the strategic hiding of patent claims.[56] There were also changes in the treatment of business methods and software, which permitted more abstract claims. Each of these factors prevents adequate notice.

In industries where patent boundaries are clear, the risks and costs of litigation are reduced due to patent notice. Chemical patents are litigated at half the rate of other patents, while financial patents are twenty-seven times more likely to be litigated that patents in other industries.[57] Litigation increases the cost of patents, and dysfunctional notice can explain increases in litigation. Also, "patent quality has declined"[58] and the decline includes hidden

---

[53] BESSEN & MEURER, *supra* note 4, at 141.

[54] *Id.* at 147.

[55] *Id.* at 164.

[56] *Id.* at 150.

[57] *Id.* at 152.

[58] BESSEN & MEURER, *supra* note 4, at 162.

claims and vague and abstractly worded claims, which decrease notice and lead to more litigation.

Chapter Eight: Small Inventors

- **Summary**: Some believe that the patent system should be judged based on the premise that small inventors benefit from the patent system, therefore making reforms unnecessary. "But the role of the small inventor is frequently hyped and distorted."[59] They are less likely to be sued because their contributions have less commercial impact.[60] Small inventors may benefit, but they also fall victim to lack of notice issues, and in the long run, their patents are less valuable than those of large firms.

- **Discussion**: One question posed is whether the inventions of small inventors are more valuable to society than those of large companies.[61] Even though inventors at small firms may have stronger incentives and large firms are slower to develop innovation that threatens the existing market, the quality of inventions of larger firms is no different than small investors.[62] However, the individual inventor is playing a lesser role than at the turn of the century.[63]

"Although individual inventors seem to be an important source for some breakthrough inventions, they are not the source of the majority of such inventions."[64] Small inventors are

[59] BESSEN & MEURER, *supra* note 4, at 166.

[60] *Id.* at 167.

[61] *Id.*

[62] *Id.* at 167-68.

[63] *Id.* at 171.

[64] BESSEN & MEURER, *supra* note 4, at 171.

more likely to work in small firms, which actually produce more relative to their size, but it does not make them more important than large firms or the inventions more valuable.[65]

Although there is some incentive to small inventors, it is much less valuable than the patents of large firms. If a small firm has depleted its cash flow, it may not be able to renew a patent; small firms also may have a greater difficulty enforcing patent rights.[66] Notice and boundary issues will also reduce the amount that a licensee is willing to pay, further reducing the value of small inventor patents. "Although patents might be critical to some small firms, they do not appear to be particularly important to most."[67]

Chapter Nine: Abstract Patents and Software

- **Summary:** Software and business method patents are extremely problematic, and incur high rates of litigation and claim review. "Software is an *abstract* technology," which creates a problem because claims are broad and obvious.[68] Because they are often abstract claims, software is not like other patents. It has been, and continues to be, more prone to litigation, primarily responsible for major patent suits and the failure of the system.[69]

- **Discussion**: Software firms opposed software patents through the mid 1990s, and software inventors have also generally been opposed to patents.[70] The concern comes from the fact that most software patents are held by firms not in the software industry because software is

[65] BESSEN & MEURER, *supra* note 4, at 172.

[66] *Id.* at 178.

[67] *Id.* at 177.

[68] *Id.* at 187.

[69] *Id.* at 213-14.

[70] BESSEN & MEURER, *supra* note 4, at 189.

widely used general purpose technology.[71] Also, "checking thousands of patents is clearly infeasible for almost any software product,"[72] which makes infringement more likely and in turn litigation, more likely.

Instead of getting better, software patent problems are getting worse and are more likely to be litigated than any other patent. This is because it is not only difficult to define the boundaries of patents, but can be close to impossible. The difficulties can be illustrated by the *Pinpoint v. Amazon* case, where Pinpoint challenged Amazon's book recommendation technology because they believed it was covered by a more general patent they held for 'collaborative filtering.'[73] Amazon argued that Pinpoint's technology was numeric, and theirs was categorical so it was not covered by Pinpoint's patent. Judge Posner agreed, however "the interpretation matched the *plain meaning* of the claim," meaning that although Amazon's technology was not numeric per se, software translates the categories into a numeric pattern.[74]

Another issue with abstract software claims is that it may cover technology that the inventor has not actually invented. "These claims reward patentees for inventions they do not invent…the actual, future inventors face *reduced* incentives."[75] The disincentive harms the actual inventors and the purpose of the patent system.

Patent law has worked to restrict abstract patents with three doctrines: subject matter doctrine, which excludes abstract subject matter like mathematics and natural law; enablement

---

[71] BESSEN & MEURER, *supra* note 4, at 190.

[72] *Id.* at 213.

[73] *Id.* at 197.

[74] *Id.* at 197-98.

[75] *Id.* at 199.

doctrine, which hold patents should provide enough information that a person skilled in the art would be able to make and use all inventions; and limits on functional claims doctrine, which authorizes and regulates the 'means-plus-function' language in abstract claims."[76] However, these have made little impact on abstract software patents.

Chapter Ten: Making Patents Work as Property

- **Summary**: Although the Federal Trade Commission and the Department of Justice have held joint hearings about the patent system and understand there is a concern, they have not been able to push through any significant reforms.[77] The reforms proposed are also unlikely to improve the system because they don't confront the notice problem

- **Discussion**: It is unlikely that today's patent system is an effective policy instrument to encourage innovation.[78] Successful patent reform may be difficult because there is so much new technology, especially in software, and to be effective patents need to do more than just provide positive incentives.[79]

"Empirical analysis has shown that poor patent notice has reduced the incentives to invent."[80] Although some notice improvements may reduce the value of some patents, the goal should be a net increase by decreasing cost and litigation, which maintaining value.[81] Property has clear boundaries, and predictable property rights require it.

---

[76] BESSEN & MEURER, *supra* note 4, at 204.

[77] *Id.* at 215.

[78] *Id.* at 216.

[79] *Id.* at 217.

[80] *Id.* at 219.

[81] BESSEN & MEURER, *supra* note 4, at 219.

"Until patents have clear, easily determined, predictably interpreted boundaries, improvements in patent quality can only have limited effect."[82] Poor patent notice limits all effectiveness. Reforms cannot be made solely to the patents, but will also require "fundamental change in the structure and functioning of the key institutions of the patent system."[83] This would target not only the Patent Office, but Courts as well making rulings more predictable. It is also suggested that the centralized patent court may not be an effective institutional arrangement. "Fundamental institutional deficiencies call for fundamental institutional change."[84] "Making patent boundaries clearer is of paramount importance" and theoretically is an improvement which consumers will also benefit from.[85]

Chapter Eleven: Reforms to Improve Notice

- **Summary**: There are three categories of notice reform: making patent claims transparent so boundary information can be obtained as soon as possible, making claims and their interpretation clear and unambiguous, and improving the feasibility of clearance search.[86] Reforms will increase the ability of an innovator to understand the scope of relevant patents, reduce clutter and clearance cost, as well as inadvertent infringement.[87]

[82] BESSEN & MEURER, *supra* note 4, at 224.

[83] *Id.* at 226.

[84] *Id.* at 231.

[85] *Id.*

[86] *Id.* at 235-36.

[87] BESSEN & MEURER, *supra* note 4, at 252-53.

- **Discussion**: Interpretive problems could solved if the Federal Circuit deferred to the interpretive tasks performed by the Patent Office and trial courts, because few judges have experience with patent cases.[88] The Patent Office could also improve notice qualities of patents and their boundaries by asking for more information about the meaning of a claim and rejecting abstract claims.[89] This would avoid unfavorable interpretation by decreasing vague claims. It is also suggested that infringement opinion letters, from the Patent Office, like those from the SEC, would be beneficial if it was given deference by the Courts.[90]

The increase in the number of patents requires reform as well. The increase has led to delays, which prolong the time claims are hidden from the public, and the workload reduces the quality of examination, increasing the number of vague claims.[91] This may be countered by stronger non-obvious standards, as well as some increases to the renewal fee, in order to reduce the patent flood.

"The act of inventing is at the heart of the patent system," therefore it is suggested that it may be a beneficial reform provide greater defense for good faith infringers.[92] The suggested defense would not be unlimited, but apply to those who began using the technology before the patent was issued.[93] A safe harbor has also been suggested for good faith infringers, because

---

[88] BESSEN & MEURER, *supra* note 4, at 238.

[89] *Id.* at 239.

[90] *Id.* at 241.

[91] *Id.* at 247.

[92] *Id.* at 243.

[93] BESSEN & MEURER, *supra* note 4, at 250.

they often do not know who they are infringing on, or when the invention occurs simultaneously, who they are racing against to acquire patent rights.

Chapter Twelve: A Glance Forward

- **Summary**: Although patents are similar to rights in tangible property there are differences in implementation.[94] The challenges to the patent system may be greater than in the past, because the systems works in some industries but fails in others. "The future of the patent system will depend on getting beyond…abstract thinking to build institutions that improve patent notice, even if this comes with realistic limits on what can be patented and how it can be claimed."[95]

- **Discussion**: The performance of the patent system depends on the details, regulations and institutions that implement the system. Real property rights have limits, and patents should as well. There has never been any "intent that the patent coverage should be expanded."[96] The property system works because there are recognized limits and boundaries, and the patent system works best in industries where patent rights are clearly defined, not abstract.

One failure of the system includes the allowing of patents on everything under the sun and the relaxed non-obvious standards, making limitations more difficult.[97] The challenge is to improve the way the patent system performs, which is becoming increasingly difficult.

---

[94] BESSEN & MEURER, *supra* note 4, at 254.

[95] *Id.* at 260.

[96] *Id.* at 255.

[97] *Id.* at 256.