UPDATES ARE NOT AVAILABLE: FDA REGULATIONS
DETER MANUFACTURERS FROM QUICKLY AND
EFFECTIVELY RESPONDING TO SOFTWARE PROBLEMS
RENDERING MEDICAL DEVICES VULNERABLE TO
MALWARE AND CYBERSECURITY THREATS

Kristy Williams .................................................................367

KNOWING IS HALF THE BATTLE: HOW LATE IS TOO
LATE TO MEET THE KNOWLEDGE ELEMENT WHEN
PLEADING INDIRECT PATENT INFRINGEMENT?

Jack Burns .................................................................418

THE ROLE OF CORPORATE INTEGRITY AGREEMENTS IN
THE EXPANSION OF FIDUCIARY DUTIES

Wulf A. Kaal and Elizabeth R. Malay.................................440

VALID BUT HARMFUL: WHY CONGRESS SHOULD
AMEND THE PATENT ACT TO INCLUDE COMPULSORY
LICENSENG OF DISEASE GENE PATENTS

Rebecca Echevarria ...........................................................464

THE USE OF TRADEMARKS AS METATAGS IN EUROPE:
EXPANDED PROTECTIONS FROM THE EUROPEAN COURT
OF JUSTICE

Emily Thornton ..............................................................487
ABOUT THE JOURNAL

The Wake Forest Journal of Business and Intellectual Property Law is a student organization sponsored by Wake Forest University School of Law dedicated to the examination of intellectual property in the legal context. Originally established as the Wake Forest Intellectual Property Law Journal in 2001, the new focus and form of the Journal, adopted in 2010, provides a forum for the exploration of business law and intellectual property issues generally, as well as the points of intersection between the two, primarily through the publication of legal scholarship. The Journal publishes four print issues annually. Additionally, the Journal sponsors an annual symposium dedicated to the implications of intellectual property law in a specific context. In 2009, the Journal launched an academic blog for the advancement of professional discourse on relevant issues, with content generated by both staff members and practitioners, which is open to comment from the legal community. The Journal’s student staff members are selected for membership based upon academic achievement, performance in an annual writing competition, or extensive experience in the field of intellectual property or business.

The Journal invites the submission of legal scholarship in the form of articles, notes, comments, and empirical studies for publication in the Journal’s published print issues. Submissions are reviewed by the Manuscripts Editor, and decisions to extend offers of publication are made by the Board of Editors in conjunction with the Board of Advisors and the Faculty Advisors. The Board of Editors works closely and collaboratively with authors to prepare pieces for publication.

Manuscript submissions should be accompanied by a cover letter and curriculum vitae, and may be sent electronically to wfujbipl@gmail.com or by mail to:

Manuscripts Editor
Wake Forest Journal of Business and Intellectual Property Law
Wake Forest University School of Law
P.O. Box 7206 Reynolda Station
Winston-Salem, North Carolina 27109

Copyright © 2014
Wake Forest Journal of Business and Intellectual Property Law

ISSN 2164-6937 (Print)
ISSN 2164-6945 (Online)
BOARD OF ADVISORS

DANNY M. AWDEH
Finnegan Henderson Farabow Garrett & Dunner LLP
Washington, DC

CHARLES W. CALKINS
Kilpatrick Townsend & Stockton LLP
Winston-Salem, North Carolina

KENNETH P. CARLSON
Constany, Brooks & Smith, LLP
Winston-Salem, North Carolina

TRIP COYNE
Williams Mullen
Wilmington, North Carolina

RODRICK J. ENNS
Enns & Archer LLP
Winston-Salem, North Carolina

EDWARD R. ERGENZINGER, JR., PH.D.
Ward & Smith, P.A.
Raleigh, North Carolina

JASON D. GARDNER
Kilpatrick Townsend & Stockton LLP
Atlanta, Georgia

STEVEN GARDNER
Kilpatrick Townsend & Stockton, LLP
Winston-Salem, North Carolina

ROB HUNTER
The Clearing House Payments Company, LLC
Winston-Salem, North Carolina

BARBARA LENTZ
Professor, Wake Forest University School of Law
Winston-Salem, North Carolina

JAMES L. LESTER
MacCord Mason PLLC
Greensboro, North Carolina

JUSTIN R. NIFONG
Olive Law Group
Cary, North Carolina

MICHAEL S. MIRELES
Professor, University of the Pacific, McGeorge School of Law
Sacramento, California

ALAN PALMETER
Professor, Wake Forest University School of Law
Winston-Salem, North Carolina

ABBY PERDUE
Associate Professor, Wake Forest University School of Law
Winston-Salem, North Carolina

COE W. RAMSEY
Brooks Pierce
Raleigh, North Carolina

T. ROBERT REHM, JR.
Smith, Anderson, Blount, Dorsett, Mitchell, & Jernigan, LLP
Raleigh, North Carolina

SIMONE ROSE
Professor, Wake Forest University School of Law
Winston-Salem, North Carolina
UPDATES ARE NOT AVAILABLE: FDA REGULATIONS DETER MANUFACTURERS FROM QUICKLY AND EFFECTIVELY RESPONDING TO SOFTWARE PROBLEMS RENDERING MEDICAL DEVICES VULNERABLE TO MALWARE AND CYBERSECURITY THREATS

Kristy Williams†

I. INTRODUCTION ................................................................. 369
   A. UPDATING COMMERCIAL OFF THE SHELF SOFTWARE TO PREVENT MALWARE INFECTION ........... 372
   B. UPDATING MEDICAL DEVICE SOFTWARE TO FIX BUGS AND RESPOND TO SECURITY THREATS .......... 373
   C. UPDATING MOBILE MEDICAL APPLICATIONS IN RESPONSE TO OPERATING SYSTEM OR DEVICE HARDWARE CHANGES ......................................................... 374
   D. UPDATING SOFTWARE ON COMBINATION PRODUCTS ................................................................. 378
   E. OUTLINE OF ARTICLE .......................................................... 378

II. FDA REGULATIONS .............................................................. 379
    A. MEDICAL DEVICES .......................................................... 380
       1. Medical Device Premarket Review ......................... 381
    B. COMBINATION PRODUCTS ............................................... 394

III. EXAMPLES AND APPLICATION ........................................... 399
    A. UPDATING COMMERCIAL OFF THE COUNTER SOFTWARE TO PREVENT MALWARE INFECTION ........ 399
    B. UPDATING SOFTWARE ON STAND ALONE MEDICAL

† Visiting Scholar, Institute for Medical Humanities, University of Texas Medical Branch. Contact: kristy.lynn.williams@gmail.com. Ph.D., Memorial University of Newfoundland; J.D., University of Calgary; LL.M., University of Houston Law Center. The author would like to thank Barbara Evans and Ronald Scott for their insights and encouragement in this research.
DEVICES IN RESPONSE TO SECURITY THREATS .......... 405
C. UPDATING MOBILE APPLICATION MEDICAL
   DEVICES IN RESPONSE TO OPERATING SYSTEM
   CHANGES.......................................................... 410
D. UPDATING SOFTWARE ON COMBINATION
   PRODUCTS........................................................... 415
IV. CONCLUSION................................................................ 417
I. INTRODUCTION

Users of electronic equipment, such as personal computers, tablets, and smartphones, are undoubtedly aware of the continual need for software updates. Updates to operating systems often spur the need for updates to other software running on the equipment. In any event, frequent updating of virus scanning software is often seen as a necessity, particularly when a computer is networked, or connected to the Internet. However, much of the software on medical devices is not updated nearly as frequently, if at all.

In the United States, medical devices are regulated by the U.S. Food and Drug Administration (“FDA”). A manufacturer generally requires permission from the FDA before a medical device can legally be marketed to the public. FDA approval or clearance to market is limited to the specific model and version of the medical device, and any later modification must be evaluated for any potential FDA approval or clearance required before the modified device is marketed. Generally, any changes affecting the safety or effectiveness of the medical device will require further FDA involvement. Even where a change has not altered the safety or effectiveness of the device, the manufacturer will have significant obligations to verify and validate the change, and potentially report to the FDA.


2 Such “permission” is obtained through the 510(k) clearance process or the premarket approval (PMA) process and is correctly referred to as clearance or approval. See INST. OF MED., MEDICAL DEVICES AND THE PUBLIC’S HEALTH: THE FDA 510(K) CLEARANCE PROCESS AT 35 YEARS 208 (2011). See infra text accompanying notes 73-74.

3 The involvement of the FDA where a change affects the safety and effectiveness of a device varies widely depending on the process through which the device was originally approved or cleared for marketing and the nature of the change. See U.S. FOOD & DRUG ADMIN., K97-1, DECIDING WHEN TO SUBMIT A 510(K) FOR A CHANGE TO AN EXISTING DEVICE 3 (1997) available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm080243.pdf [hereinafter FDA 510(K) CHANGES]; PMA Supplements and Amendments, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050467.htm (last updated Mar. 18, 2014) [hereinafter FDA PMA CHANGES].

4 See FDA PMA CHANGES, supra note 3; FDA 510(K) CHANGES, supra note 3.

5 21 C.F.R. § 820.20 (2013) (describing FDA regulations implementing Quality Systems); 21 C.F.R. § 806.10(a)(1) (2013) (describing the obligation to report changes where the change is taken to reduce a risk to health); see infra text continued . . .
Medical devices are becoming increasingly technical and complex, with many containing software as a part of the final product. Devices can contain both proprietary software, as well as commercial off-the-shelf (“COTS”) software, such as the Windows operating system. The software in medical devices, like all software, has the potential to contain errors that affect the functionality of the device and potentially expose the device to cybersecurity threats. Furthermore, unlike in traditional engineering, a minute error in software coding can have a huge impact. When a manufacturer discovers a software vulnerability in its medical device, the manufacturer is not necessarily obligated to remedy the vulnerability. Such vulnerabilities are primarily addressed through the issuance of software updates; however, a software update is considered a change in the medical device, and therefore must be evaluated to determine what obligations the manufacturer has under FDA regulations, including whether further FDA involvement is required. Some software engineers take the position that the need for software updates would be significantly reduced by an overhaul in the way that software is designed for medical devices. It is argued that the medical device industry should follow the well-known techniques for critical systems.
in the avionics industry where the adoption of more secure technology has been successful.\textsuperscript{12} Regardless of whether such an overhaul is the most favorable approach, or is even feasible, software updates will likely be required to address software vulnerabilities of medical devices that are currently marketed. In any event, if medical device software is eventually redesigned, at least some of the overhauled software will come to market through the FDA’s process for approving or clearing changes to medical devices.

For over two decades, the FDA has recognized that the use of software in medical devices adds a point of vulnerability.\textsuperscript{13} The FDA has therefore taken steps through regulations to mitigate such vulnerabilities.\textsuperscript{14} However, due to the complexity and perceived effort required to get updates approved, as well as the risk of an updated device being unmarketable, the FDA’s complex regulations disincentivize manufacturers from issuing software updates.\textsuperscript{15} Moreover, the FDA has recognized that while revisions to software are important, these revisions are a major source of software related device problems, and therefore careful control of software revisions is required.\textsuperscript{16}

\begin{footnotesize}
\begin{enumerate}
\item Fu, \textit{supra} note 6, at 103-06. The author’s suggestions draw from software engineering for critical systems and include: adopting modern software engineering techniques to reduce or eliminate common sources of software errors, specify meaningful requirements such as adding functionality in a dosing device to stop administering drugs once the patient’s prescription has been exceeded, apply a systems engineering approach including testing the software in the system environment in which it will be integrated and not as an isolated component, mitigate risks due to human factors, and mitigate low-probability high consequence risks brought on by medical professionals having too much confidence in device software. See Fu, \textit{supra} note 6, at 103-06.
\item See \textit{Recalls, Corrections and Removals (Devices), supra} note 13 (discussing recalls as methods of “removing or correcting products that are in violation” of FDA laws which would mitigate vulnerabilities by protecting the public health).
\end{enumerate}
\end{footnotesize}
Although a cautious approach to updating medical device software is appropriate, care must be taken to ensure that manufacturers do not stop providing updates, particularly when problems involving the device are identified. This article will focus on the following four areas where updates are needed to address software vulnerabilities in medical devices: (1) updating COTS software to prevent virus and malware infection; (2) updating medical device software to fix bugs and respond to security threats; (3) updating mobile medical applications in response to operating system or device hardware changes; and (4) updating software on combination products.

A. Updating Commercial Off the Shelf Software to Prevent Malware Infection

Given the frequency with which we update our computers and personal devices, it is difficult to imagine the performance of a medical device being continually impaired where there is an available, although not necessarily accessible, solution. However, there are numerous instances where the functionality of medical devices have been negatively impacted by malware when commercially available security patches or anti-virus software were not installed or updated.

The Office of Information Security for the Department of Veterans’ Affairs (“VA”) found 142 separate malware infections infecting 207 medical devices in a variety of departments in VA hospitals from 2009 to 2011.17 The most common result of malware was the inability to provide patient care due to computer outages; for example, in one extreme instance, patients had to be transported to a different hospital.18 Similarly, medical devices routinely become infected with malware at Beth Israel Deaconess Medical Center in Boston.19 Most of the affected devices run on embedded Windows

problems . . . happen to devices that are running software that has been revised since premarket review.”).


18Id.

operating systems, for which the manufacturers say that the users cannot patch or install virus software due to the devices being 510(k) cleared. As a result, malware accumulates on the unsecured devices in under twelve days, compared to the over 300 days it takes for other systems in the Medical Center running anti-virus software and security patches. The specific effects of malware are device dependent; for instance, when devices used to monitor high-risk pregnancy were compromised, the devices still displayed data in real time during use but failed to record the data. A further example of malware protection being negatively affected by FDA regulations perceived to be overly complicated was the infection of 300 critical medical devices from a single manufacturer at medical centers across the United States and the globe with the Conficker Virus. The discoverers of the infections were told, by device manufacturers, that regulations required ninety-days’ notice before the device could be modified to remove the infections and vulnerabilities. This suggests that the manufacturer believed that updates to remove infections and remedy vulnerabilities required a new FDA clearance.

B. Updating Medical Device Software to Fix Bugs and Respond to Security Threats

As the complexity of medical device software increases, so does the occurrence of vulnerabilities. One such vulnerability that has

CISO of Beth Israel Deaconess Medical Center describing the malware issues faced by the 905 devices on the wired network and 2,000 wireless devices).

20 Id.
21 Id.
22 Id.
24 Id.
25 A manufacturer is required to give the FDA 90 days notice before marketing a new or changed medical device that requires a new 510(k) clearance; see Federal Food, Drug, and Cosmetics Act § 510(k), 21 U.S.C. § 360(k) (2012) (“Each person who is required to register under this section and who proposes to begin the introduction or delivery for introduction into interstate commerce for commercial distribution of a device intended for human use shall, at least ninety days before making such introduction or delivery, report to the Secretary or person who is accredited under section 360m(a) . . . ”).
26 See Shane S. Clark & Kevin Fu, Recent Results in Computer Security for Medical Devices, 2011 INT’L ICST CONFERENCE ON WIRELESS MOBILE COMM’CN AND HEALTHCARE (MOBIHEALTH), available at https://spqr.eecs.umich.edu

continued . . .
gained recent attention is devices, particularly wireless devices, becoming cybersecurity targets.\textsuperscript{27} It has been demonstrated that insulin pumps and pacemakers are vulnerable to hacking, wherein the function of the device may be manipulated to give the user a lethal shock or dose of insulin.\textsuperscript{28} In addition to direct hacking of medical devices, it has been posited that medical devices may also be vulnerable to malware infection, which have the potential to impact the operation of the device in ways similar to hacking.\textsuperscript{29}

C. Updating Mobile Medical Applications in Response to Operating System or Device Hardware Changes.

Medical Devices are increasingly incorporating smartphones or tablets,\textsuperscript{30} commonly referred to as mobile medical applications or mobile medical apps.\textsuperscript{31} In its September 2013 Guidance, the FDA


\textsuperscript{29} Clark & Fu, supra note 26, at 4 (stating that one research group showed that a stuxnet worm was able to seek out a specific programming language while another group has successfully loaded custom software onto an AED, demonstrating the potential for a self-replicating work to infect an AED and spread to other AED’s).

\textsuperscript{30} The use of mobile health applications has been exponentially increasing in recent years and are expected to continue to increase. See Ralf-Gordon Jahns, 500m people will be using healthcare mobile applications in 2015, RESEARCH2GUIDANCE (Nov. 20, 2010), http://www.research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/.

\textsuperscript{31} For the remainder of this article “mobile medical apps” refers to applications continued . . .
stated that it would regulate mobile medical apps that meet the definition of “device” in section 201(h) of the Federal, Food Drug and Cosmetic Act, and that are either intended to (1) “be used as an accessory to a regulated medical device;” or (2) “transform a mobile platform into a regulated medical device.” Mobile medical devices exist in different forms including: entirely as software on the mobile platform (such as Astra imaging software, Aycan mobile software, and Prodigy diabetes management software), or as software with accompanying hardware that attaches to or interacts with the mobile platform (such as the iExaminer to take images of the eye, Mobius ultrasound imaging system, AliveCor heart monitor, which uses a case for the iPhone as leads, iBGStar blood glucose monitor, which
connects to iPhone, and iHealth blood pressure monitor\(^{41}\)). Due to the platforms on which they operate (i.e., the tablet or smartphone), mobile medical apps face unique challenges as opposed to other medical devices containing software. For traditional medical devices, manufacturers specify the operating system requirements and under FDA regulations users are prevented from upgrading or making changes to the software or hardware without the manufacturer’s approval.\(^{42}\) It is apparent that users, particularly medical professionals or those working for large medical centers, follow these requirements in order to comply with the FDA.\(^{43}\) Users of mobile platforms do not have as much flexibility as to what version of operating system their device is running. Mobile platform operating systems are constantly being updated, and it is very easy for a user to mistakenly update the operating system to an unsupported version, with little ability to revert to the prior version.\(^{44}\) Additionally, users may download purchased

---

\(^{30}\) pin connector).

\(^{41}\) FDA Premarket Notification Database, iHealth BP3 Fully Automatic Arm Cuff Electronic Blood Pressure Dock K102939, FDA (Feb. 23, 2011), http://www.accessdata.fda.gov/cdrh_docs/pdf10/K102939.pdf (describing a blood pressure monitor that connects to an iPhone, iPod or iPad).

\(^{42}\) This is necessary because according to FDA regulation, a premarket notification submission is required by a manufacturer when a device is being introduced into interstate commerce for commercial distribution that is intended for human use and is significantly changed or modified. See 21 C.F.R. § 807.81(3) (2013) (“the device is one that the person currently has in commercial distribution or is reintroducing into commercial distribution, but that is about to be significantly changed or modified in design, components, method of manufacture, or intended use. The following constitute significant changes or modifications that require a premarket notification: (i) A change or modification in the device that could significantly affect the safety or effectiveness of the device, e.g., a significant change or modification in design, material, chemical composition, energy source, or manufacturing process.”).

\(^{43}\) Users appear to go to great lengths to downgrade systems to comply with manufacturer’s system requirements. See Kevin Fu, Trustworthy Medical Device Software, 2011 MIT CSAIL SEMINAR Slide 40, available at http://web.eecs.umich.edu/~kevinfu/talks/Fu-med-MIT-2011.pdf (exhibiting a screenshot from an IT help form where a user commented “[b]efore you post it would be wise to ask why the computer needs to be downgraded. I am setting up a medical imaging facility and I am trying to do the same thing as well. The PACS system we are integrating with is only compatible with SP2. I order 6 new Dell workstations and they came preloaded with SP3 . . . [y]ou stated ‘if you installed XP with integrated sp3, it is not possible to downgrade sp3 to sp2,’ is this true? Do you have any supporting documentation as this would be very helpful so that I can provide Dell with a reason why I need to order downgraded XP discs.”).

apps onto any model of a mobile platform that they own and many users routinely upgrade to the newest hardware model of the platform as it becomes available.\textsuperscript{45} Newer models generally have hardware changes such as different processors, cameras, display features, and physical sizes.\textsuperscript{46} Their differences will become increasingly important where the mobile medical app relies on the smartphone hardware such as the camera.

For example, the mobile medical application AliveCor Heart Monitor for iPhone, is an electrocardiogram cleared for marketing by the 510(k) process.\textsuperscript{47} In 2013, the application was approved for use with iPhone 4 or 4s,\textsuperscript{48} and the manufacturer was working on having a comparable device for the iPhone 5 cleared by the FDA.\textsuperscript{49} It is likely that the manufacturer required this clearance because the device includes ECG leads that must connect to an iPhone case, and the iPhone 5 is a physically different size than the iPhone 4.\textsuperscript{50} So there were manufacturing differences required for the device to be compatible with the new platform model. However, multiple reviewers indicated they were using the app with an iPad\textsuperscript{51} (an

\textsuperscript{45} See generally id.

\textsuperscript{46} See U.S. FOOD & DRUG ADMIN., supra note 31, at 6-7 (“Certain mobile medical apps may pose risks that are unique to the characteristics of the platform on which the mobile medical app is run. For example, the interpretation of radiological images on a mobile device could be adversely affected by the smaller screen size, lower contrast ratio, and uncontrolled ambient light of the mobile platform.”).

\textsuperscript{47} FDA Premarket Notification Database, supra note 39.

\textsuperscript{48} Mark Wilson, This $200 iPhone Case Is An FDA-Approved EKG Machine, FASTCODESIGN.COM (Dec. 5, 2012, 7:45 AM), http://www.fastcodesign.com/1671371/this-200-iphone-case-is-an-fda-approved-ekg-machine.

\textsuperscript{49} Id.

\textsuperscript{50} Ben Reid, iPhone 4 Compared With iPhone 5 Case, Shows Significant ‘Thinness’ in Design, REDMONDPIE.COM (Sept. 3, 2011), http://www.redmondpie.com/iphone-4-compared-with-iphone-5-case-shows-significant-thinness-in-design-photo/.

\textsuperscript{51} OMMD, Works well with my iPad one!, METRICSAT (Feb. 2, 2013), http://iphone.metricscat.com/aliveecg/is_short/long/page/2/ (reviewing AliveCor Heart Monitor App) (“To all of you iPhone 5 owners, I’m guessing it should be an easy upgrade for the company as this device already works with my iPad one! It might be a matter of FDA approval as it is definitely not a technical matter. With the iPad however it needed to be closer. If you place the device and the back of your iPad and hold it you’ll get the same ECG rhythm you get on the iPhone.”); BigRed1010, Great App – But Requires Accompanying Hardware, METRICSAT (Mar. 13, 2013), http://iphone.metricscat.com/aliveecg/is_short/long/page/2/ (reviewing AliveCor Heart Monitor App) (“This app requires hardware so please don’t rate unless you have both. If you do, you do a disservice to both users and

\textit{continued...}
unapproved model) suggesting that app users are less likely to comply with regulatory requirements than users of traditional medical devices. Reports of similar unapproved use were also seen with the iBGStar Glucose monitor, which attached to the iPhone via the Apple 30 pin connector. Users reported through reviews on the Apple App Store that they were using the device with an iPhone 5 (which does not have a 30 pin connector) by using an adaptor that converts the lightning port to a 30 pin connector.

D. Updating Software on Combination Products

Another potential source of confusion is determining what regulations govern the updating of software where the software is part of a combination product. Advances in technology have resulted in many combination products that are part device and part drugs, such as a pacemaker with drug effusing leads. Regulation of software updates for software on the combination product will particularly be complicated where the primary mode of operation of the product has been held to be a drug, and therefore the changes are being regulated not by the CDRH but by the CDER.

E. Outline of Article

This Article is structured as follows: Part II provides necessary background on the FDA’s current regulatory scheme affecting programmers. We purchased one for testing. It works surprisingly well, and although it says it only works for the iPhone 4/4s, it’s because they designed the hardware into a 4/4s case. We tested it using an iPad. It works as long as you hold it close. I’m sure it would work just fine for the iPhone 5, it just wouldn’t fit in it. For the iPad, we ran the sister program Veterinary Alive ECG.”). Heywardjr, Please update the device with a lightning connector!, SENSOR TOWER (Dec. 11, 2013), https://sensortower.com/ios/us/sanofi-aventis-us-llc/app/ibgstar-r-diabetes-manager/506018173 (reviewing iBGStar Diabetes Manager App) (“I’m a bit surprised that this device is still using the oh-so-dated 30-pin connector.”).

Mafutha, Works great with iPod 5th, METRICS CAT (Mar. 26, 2013), http://iphone.metricscat.com/ibgstar-diabetes-manager/ (reviewing iBGStar Diabetes Manager App) (“Work[s] well with my iPod 1g but also works with my iPod 5g. I use the lightning to 90-pin connector and it work[s] great.”).


II. FDA Regulations

The Federal Food, Drug and Cosmetics Act gives the FDA the power to regulate items falling in the following four categories of products: drug, device, biological product, and combination product. Regulation of these products is facilitated by the Center for Drug Evaluation and Research (“CDER”), the Center for Biologics Evaluation and Research (“CBER”), the Center for Devices and Radiological Health (“CDRH”), and the Office of Combination Products (“OCP”).

This article will focus on the FDA’s regulation of medical devices pertaining to software updates. However, in recognition of the fact that the technology of medical devices is ever expanding, resulting in such devices increasingly falling under the category of combination products, the regulation of changes to combination products will also be discussed.

---

57 Id.
59 21 C.F.R. § 3.2(e)(1) (2013) (defining a combination product as a “product comprised of two or more regulated components, i.e., drug/device, biologic/device, drug/biologic, or drug/device/biologic, that are physically, chemically, or otherwise combined or mixed and produced as a single entity.”).
60 This discussion will focus on the regulation of changes to the software component of the combination device.
A. Medical Devices

The FDA is empowered to regulate the use of medical devices pursuant to section 321(h) of the Federal Food, Drug, and Cosmetic Act. A medical device is defined as:

[A]n instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—

. . . (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, . . . or

(3) intended to affect the structure or function of the body.

Medical devices may be solely composed of software or contain one or more software components, parts or accessories, and the software contained in such a device is subject to FDA regulation. For the purpose of this article, such software containing devices will be referred to as “software devices” and include firmware and other means for software-based control of medical devices, standalone software applications such as mobile applications, software intended for installation in general purpose computers, dedicated hardware or software medical devices, and accessories to medical devices when those assessors contain or are composed of software. Software devices are regulated in the same manner as other medical devices.

The FDA's regulatory scheme for medical devices involves: a risk stratified three tiered approach for the introduction of new medical products to the market as well as various post-market regulations including requirements to continually verify and validate the device and make changes when required. This regulatory scheme is implemented by the CDRH.

Medical devices are required to be placed into one of three classes,
with the classification generally being determined on the risk associated with the device and the level of regulatory control needed to provide reasonable assurance of safety and effectiveness. General controls apply to all classes of devices and include: prohibitions on contamination, false or misleading labeling, and a device being unsafe when used in accordance with instructions; and mandates on registration, listing of products, label information, design and manufacture of products, reports of removals and corrections, and reporting of adverse medical events. Class I devices are devices for which general controls are sufficient to provide reasonable assurance of safety and effectiveness. Class II devices are devices for which general controls alone are insufficient and for which there is sufficient information to establish special controls to provide assurances of the safety and effectiveness of the device. Class III devices are devices for which general controls are insufficient and for which there is insufficient information to establish special controls to provide reasonable assurances of safety and effectiveness.

I. Medical Device Premarket Review

In general, the classification of a device governs the type and extent of FDA review before the device enters the market (premarket review) with Class III devices being subject to the most intense scrutiny and Class I devices being exempted from review. Class II devices primarily proceed through the premarket notification process (more commonly referred to as 510(k) clearance), although some Class II devices have been exempted from 510(k) review and proceed to market similar to Class I devices. Most Class III devices are subject to premarket approval ("PMA"), however 25 types of Class III devices are eligible for the 510(k) clearance.

68 CTR. FOR DEVICES & RADIOLOGICAL HEALTH, supra note 7, at 21.
71 Id. §§ 360c(a)(1)(B); 513(a)(1)(B).
72 Id. §§ 360c(a)(1)(C); 513(a)(1)(C).
73 The FDA Modernization Act of 1997, Pub. L. No. 105-115, 830 Stat. 44, gave the FDA the authority to directly exempt Class II devices; on Jan 21, 1998, the FDA published a list of Class II devices that no longer require premarket notification. See Medical Devices; Exemptions from Premarket Notification; Class II Devices, 63 Fed. Reg. 3142 (Jan. 21, 1998).
74 CTR. FOR DEVICES & RADIOLOGICAL HEALTH, supra note 7, at 23; INST. OF MED., supra note 2.
The FDA’s May 2005 Guidance for Industry discusses the contents of premarket submissions and application for software devices and set out a number of common elements of such applications.\(^75\) Firstly, such submissions and applications generally require a description of the device design including an overview of device features controlled by software as well as information on the programming language, hardware platform, operating system and use of COTS software.\(^76\) Secondly, software device submissions and applications should include an analysis of potential device hazards including identification of foreseeable hazardous events, the potential severity of the events, how such events may be caused, and controlled, and possible corrective measures that have been taken.\(^77\) Finally, software device applications and submissions should also contain information demonstrating traceability, linking together design, implementation, testing and risk management.\(^78\) In any event, the exact types of documentation required depends on the type of clearance or approval being sought and an estimate of the injury that the device could permit or inflict.\(^79\)

\textit{a. Premarket Notification (510(k) Clearance)}

510(k) clearance was originally adopted in 1976 as a transitional tool to assist the coming into force of medical device regulations and the achievement of regulatory parity between pre and post-1976 devices.\(^80\) 510(k) clearance has since evolved into a permanent means for the premarket review of new devices.\(^81\)

510(k) clearance relies on the determination that the new device is \textit{substantially equivalent} to a legally marketed device that does not require premarket approval.\(^82\) The clearance process begins with the sponsor of a new device submitting a notice to the FDA setting forth the device’s proposed intended use or indications for use, the device to which substantial equivalence is claimed, and evidence demonstrating

\(^{75}\) U.S. \textit{Food & Drug Admin.}, supra note 16, at 5.

\(^{76}\) U.S. \textit{Food & Drug Admin.}, supra note 16, at 11.

\(^{77}\) U.S. \textit{Food & Drug Admin.}, supra note 16, at 11.

\(^{78}\) U.S. \textit{Food & Drug Admin.}, supra note 16, at 8.


\(^{80}\) \textit{Inst. of Med.}, supra note 74, at 86-87.

\(^{81}\) \textit{Inst. of Med.}, supra note 74, at 86-87.

\(^{82}\) \textit{See} Food and Drug Admin. Premarket Notification Procedures, 21 C.F.R. § 807.92(a)(3) (2013) (a legally marketed device is a device that was legally marketed prior to May 28, 1976, for which a PMA is not required or a device which has been reclassified from Class III to Class II or I or a device which has been found to be substantially equivalent through the 510(k) process).
the equivalence. 83 A manufacturer is required to submit such premarket notice ninety days prior to beginning to market the device. 84 Clearance to market the device is obtained only when the submitter receives an order (letter) from the FDA which finds that the device to be substantially equivalent. 85

The term substantial equivalence was not defined in the original 1976 medical device regulations, and, as a result, the term was used broadly to clear many novel devices as well as the computerization and technological advancement of many devices under the 510(k) clearance pathway. 86 Substantial equivalence has since been defined in the Safe Medical Devices Act of 1990, 87 which provided that a device is equivalent if, in comparison to a predicate, it has the same intended use and has: (1) the same technological characteristics as the predicate, or (2) different technological characteristics as the predicate and information submitted to the FDA does not raise new questions of safety and effectiveness and demonstrates that the device is at least as safe and effective as the legally marketed device. 88

b. Premarket Approval

High-risk medical devices that pose a significant risk of illness or injury and that are not substantially equivalent to Class I or II devices, and thus not eligible for 510(k) clearance, may only be offered for sale in the United States if PMA has been obtained from the FDA. 89 PMA is more complex than 510(k) clearance and requires valid scientific evidence including clinical data to support claims made about the device and prove that the device is safe and effective for its intended

---

84 Federal Food, Drug, and Cosmetics Act § 510(k); 21 U.S.C. § 360(k) (2012) (“Each person who is required to register under this section and who proposes to begin the introduction or delivery for introduction into interstate commerce for commercial distribution of a device intended for human use shall, at least ninety days before making such introduction or delivery, report to the Secretary or person who is accredited under section 360m(a). . . ”).
85 Id. § 513(i), 21 U.S.C. § 360c(i) (2012).
86 INST. OF MED., PUBLIC HEALTH EFFECTIVENESS OF THE FDA 510(K) CLEARANCE PROCESS: BALANCING PATIENT SAFETY AND INNOVATION 22-28 (2010); INST. OF MED., supra note 2, at 208.
88 21 U.S.C. § 360c(i)(1); see CTR. FOR DEVICES & RADIOLOGICAL HEALTH, supra note 7, at 27 (decision making tree for device substantially equivalence).
use. Specifically, the PMA application must include: full reports of all information known to or reasonably known to the applicant regarding investigations to assess the safety and effectiveness of the device; a full statement of the components and properties of the device and of the principles of its operation; a full description of the methods used in, and the facilities and controls used for its manufacture, processing, and packaging and installation; specimens of the labeling proposed to be used for the device; and any other information relevant to the PMA application that the FDA may require.

Approval to market the device is only available after the FDA grants a PMA approval order. The FDA may impose post-approval requirements in a PMA approval order, including the obligation to make periodic reports of certain device changes.


a. Quality Systems

With the exception of some Class I medical devices, all medical device manufacturers are obligated to follow current good manufacturing practices (CGMP’s) and establish quality systems through which they can detect flaws, including quality and design problems. The current CGMP Rule became effective June 1, 1997, and does not prescribe specifically how a specific device must be produced; however, the regulations do set out a framework by which a

---

90 Id. § 515(c), 21 U.S.C. § 360e(c).
91 Id.; 21 C.F.R. § 814.20 (2013) (detailing the required content and format of a PMA).
92 C.F.R. § 814.44(d).
93 21 C.F.R. 814.39(e) (2013); 21 C.F.R. § 814.82(a) (conditioning FDA’s approval on the fulfillment of a broad list of postapproval requirements); 21 C.F.R. § 814.84(b) (setting forth requirements for periodic reports).
manufacturer can develop their own quality system. In enacting these regulations the FDA specifically recognized the need for the application of quality systems to the software components of medical devices, and extended the application of quality system requirements to the manufacturers of these components (where they are produced separately from the rest of the device) as well as to device manufacturers.

A major component of a quality system is the establishment of design controls and the implementation of procedures to detect, prevent, and correct quality problems. Manufacturers of Class II and Class III devices as well as listed Class I devices are subject to design control regulations and are thereby obligated to establish and maintain procedures to control the design of the device in order to ensure that specific design requirements are met. Some of the design controls that are particularly applicable to software devices require implementing procedures for design verification, design validation, and design changes, as well as maintaining a design history file where results of design validation are recorded. Design verification requires “confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.” Design validation requires manufacturers to ensure that devices conform to intended uses and user needs and includes code inspections to confirm that the software output meets its input requirements. Design validation requires manufacturers to ensure that devices conform to intended uses and user needs and includes

---

96 21 C.F.R. § 820; Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule 61 Fed. Reg. 52,602, 52,603 (Oct. 7, 1996) (to be codified at 21 C.F.R. pts. 808, 812 and 820) (“...the regulation provides the framework that all manufacturers must follow by requiring that manufacturers develop and follow procedures and fill in the details that are appropriate to a given device according to the current state-of-the-art manufacturing for that specific device.”).

97 Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule 61 Fed. Reg. at 52,606 (Quality must be built into medical devices through the use of quality systems, as the complexity of software results in testing of the finished device not always being adequate).

98 21 C.F.R. §§ 820.100; 21 C.F.R. § 820.30; Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule, 61 Fed. Reg. at 52,607 (with respect to 21 C.F.R. § 820.100 “This section requires manufacturers to establish procedures to identify quality problems and process the information received to detect and correct quality problems.”).

99 Listed Class I devices include “devices automated with computer software”, therefore all devices containing computer software are subject to design controls.

100 21 C.F.R. § 820.30(a).

101 21 C.F.R. § 820.20(g), (i), (j).

102 21 C.F.R. § 820.3(aa).

103 U.S. FOOD & DRUG ADMIN., supra note 16, at 3.
software validation and risk analysis, where appropriate. In its May 2005 Guidance to Industry, the FDA noted that software validation “involves checking for proper operation of the software in its actual or stimulated use environment, including integration into the final device where appropriate”, and further that such validation is dependent on software testing and verification throughout the software development process.

Manufacturers are also required to establish procedures for the identification, documentation, verification, validation, review, and approval of design changes before their implementation. The FDA noted in preamble to the CGMP Rule, that where changes are made to the device, the manufacturer is obliged to evaluate such changes to determine whether they are obliged to submit a 510(k) clearance or file a PMA supplement. The obligation to evaluate such changes applies regardless of the reason for the changes and therefore applies whether such changes are made preemptively, in response to current problems or to add additional features. Quality system regulations thus impose an obligation on manufacturers to verify and validate all software changes before they are implemented regardless of how minor the change. The extent of the change would likely only impact the extent of verification necessary, for instance the FDA has suggested that most software changes for the purposes of addressing malware cybersecurity vulnerabilities wouldn’t require clinical validation. It is of note that quality systems are an internal process and do not require any FDA involvement.

b. Changes Requiring FDA Involvement: 510(k) Clearance or PMA supplement

When a manufacturer modifies a legally marketed device, the manufacturer must evaluate the change to determine if further

---

104 21 C.F.R. § 820.3(z)(2); 21 C.F.R. § 820.30(g).
106 21 C.F.R. § 820.30(i).
108 Id.
110 Id. at 5.
approval or clearance is required. Generally a device that has already proceeded to market via 510(k) clearance or PMA will remain in the same clearance or approval pathway. However, manufacturers of devices must be cognizant of whether the changes they have made are significant enough to effect the device classification and therefore change the required clearance or approval method. For example, consider the situation where a manufacturer of a 510(k) cleared insulin pump makes a software modification to change the functionality of the device. The manufacturer needs to consider whether the change requires a new 510(k) submission or alternatively whether the change is so significant that the device is no longer substantially equivalent to a predicate device and must proceed to market via a PMA.

i. New 510(k) Submission (Traditional and Special)

When a 510(k) cleared medical device is modified there are four possible routes through which the changed device may proceed to market: (1) premarket approval; (2) traditional 510(k) clearance; (3) special 510(k) clearance; or (4) proceed directly to market with no approval required.

PMA is required where the change or modification results in the device no longer being substantially equivalent to a predicate device, such as described in the insulin monitor example above.

In order for a change in a legally marketed medical device to require a new 510(k) submission two criteria must be fulfilled. First, the medical device must be one for which 510(k) clearance is required; meaning that the device is not exempt from clearance or requires premarket approval.

Second, the medical device must either have a major change in its intended use or a change/modification that could


112 In order to result in the device no longer being substantially equivalent to a predicate device, the software change would have to result in a significant change, such as if it resulted in the pump no longer being used to treat diabetes, but some other disease.

113 See FDA 510(K) CHANGES, supra note 3, at 3-8.


115 21 C.F.R. § 807.20(a) (2013) (“Who must register and submit a device list”); FDA 510(K) CHANGES, supra note 3, at 15 (explaining even if a changed device is exempt from the requirement to submit a 510(k) still need to evaluate the change to ensure that it does not effect the device’s classification or exemption status).
significantly affect the safety or effectiveness of the device.116 Such changes may include modifications in design or components, including changes or modifications to the material, chemical composition, or energy source.117 The FDA has intimated that a change in software may raise new issues of safety and effectiveness where routine validation activities (implemented under the CGMPs) produce unexpected results or are otherwise inadequate in validating design changes requiring new 510(k) clearance.118 The FDA further indicates that a 510(k) submission may be required where a significantly different testing scheme is required to validate the changed design.119

If the change in the medical device meets the two above listed criteria, 510(k) clearance is required and may proceed via two methods, traditional 510(k) clearance or special 510(k) clearance.120 Traditional 510(k) clearance is the same as the clearance required for the original clearance of the device, as described above, and requires that the FDA find that the device is substantially equivalent to a legally marketed device.121 However, special 510(k) clearance is an abbreviated process that is only available for device modification where the modification does not affect the intended use or alter the fundamental scientific technology of the device.122 Special 510(k) clearance relies on the assurances of quality provided by quality systems regulations.123 All that is required for special 510(k) clearance is that manufacturers comply with their quality system obligations and submit documentation related to the modification that prompted the submission.124

---

116 21 C.F.R. § 807.81(a)(3). See also FDA 510(k) CHANGES, supra note 3, at 15 (a new 510(k) should be submitted where a change affects the indications for use such as “changing the length of a surgical scissor from 10 centimeters to 30 centimeters so that the device could be used in laparoscopic procedures.”).
118 See FDA 510(k) CHANGES, supra note 3, at 16.
119 FDA 510(k) CHANGES, supra note 3, at 16.
121 Id.
122 Id. at 4.
123 CTR. FOR DEVICES & RADIOL. HEALTH, supra note 120 (quality system regulations include design control, verification and validation requirements to reduce amount of information that a manufacturer is required to provide in the submission itself).
124 U.S. FOOD & DRUG ADMIN., GUIDANCE FOR THE CONTENT OF PREMARKET SUBMISSIONS FOR SOFTWARE CONTAINED IN MEDICAL DEVICES 16 (2005), available continued . . .
indicated that it should be appropriate for software modifications to be reviewed through special 510(k) clearance.\textsuperscript{125}

What specific pathway a manufacturer should take when making a change to their legally marketed 510(k) medical device depends on the effect of the change. Where the change does not affect the intended use or the safety and effectiveness of the device, the manufacturer does not need to make a 510(k) clearance submission, and must merely comply with its reporting obligations as well as quality system obligations of testing, validating and recording.\textsuperscript{126} Where there has been a change in the intended use of the device the manufacturer must obtain clearance through a traditional 510(k) submission before marketing the changed device. Where the change may significantly affect the safety and effectiveness of the device but not the fundamental scientific technology the manufacturer may obtain clearance through a special 510(k) clearance, however, where the scientific technology of the device has been altered a 510(k) clearance is required.

\textit{ii. PMA Approved Devices}

A modified PMA medical device may proceed to market through numerous routes including: various types of PMA supplements, thirty-day notice, periodic report,\textsuperscript{127} or a new PMA. The appropriate pathway for approval depends upon the type of change being effected, with the most significant changes requiring a whole new PMA application, minor changes not requiring approval at all but merely to be reported to the FDA in a periodic report, and changes that fall in between requiring the submission of a PMA supplement.\textsuperscript{128}

A new PMA must only be obtained prior to the marketing of a changed medical device, where the modifications to the approved

\textsuperscript{125} CTR. FOR DEVICES & RADIOLOGICAL HEALTH, supra note 120, at 7 (software modifications were included in a list of device modifications that would not result in changes in fundamental scientific technology and therefore would be appropriate for special 510(k) review). A change in software can further be distinguished from examples given by the FDA, supra as to where there would be a change in fundamental technology which included a change in a surgical instrument that uses a sharpened metal blade to one that cuts with a laser and incorporation of a sensing mechanism in a device to allow the device to function “on demand” rather than continuously.

\textsuperscript{126} For quality system obligations see supra notes 94 - 126 and associated text; for reporting obligations see infra notes 152-155 and associated text.

\textsuperscript{127} 21 C.F.R. § 814.39 (2013).

\textsuperscript{128} FDA PMA CHANGES, supra note 3.}
PMA device result in a new device. 129 A new device includes one that treats a different population of patients, has a different intended use, or has a different mode of operation and therefore the preclinical and clinical data submitted in the original application is not applicable to demonstrate the safety and effectiveness of the changed device.130 For device modifications affecting the safety and effectiveness131 of a medical device, a manufacturer is required to file a PMA supplement or thirty-day notice.132 There are four types of PMA supplements: (1) special PMA supplement; (2) panel-track supplement; (3) 180-day supplement and (4) real-time supplement.133 Both the special PMA supplement134 and the thirty-day notice requirement135 apply to select


130 FDA PMA CHANGES, supra note 3 (providing that a new PMA application is required where “the design change causes a different intended use, mode of operation, and technological basis of operation.”).

131 21 C.F.R. § 814.39(a) (providing examples of changes that will affect the safety and effectiveness of a device and trigger the need for a PMA supplement include: new indications for use of the device; changes in manufacturing facilities, methods, or quality control procedures; and changes in the performance or design specifications, circuits, components, ingredients, principles of operation or physical layout of the device).


133 FDA regulations set out two specific types of PMA supplements: special PMA supplements and 30-day Notice/135 PMA supplement; the regulations also set out a general type of PMA supplement. 21 C.F.R. §§ 814.39(c), (d)(1), (f). Three additional types of PMA supplements are defined in the Federal Food Drug and Cosmetics Act, Section 737(4), as codified, including the: panel-track supplement, 180-day supplement, and real-time supplement. 21 U.S.C. §§ 379i(4)(B)-(D) (2012).

134 A special PMA supplement may be filed where the changes have enhanced the safety of the device or the safety in the use of the device by improving the labeling of the device or adding new tests to the quality controls or manufacturing of the device. See 21 C.F.R. § 814.39(d)(2). The modified device may be marketed and subject to some limitations, prior to FDA’s approval of the supplement. See 21 C.F.R. § 814.39(d)(1).

135 21 C.F.R. § 814.39(f) (providing that the thirty-day notice and 135 PMA supplement may only be used where change have been made in the device’s manufacturing process, as the procedure permits the manufacturer to make manufacturing changes thirty days after giving notice to the FDA); U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY AND FDA STAFF: 30-DAY NOTICES, 135-DAY PREMARKET APPROVAL (PMA) SUPPLEMENTS AND 75-DAY HUMANITARIAN DEVICE EXEMPTION (HDE) SUPPLEMENTS FOR MANUFACTURING METHOD OR PROCESS CHANGES 7 (2011), available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM080194.pdf (providing that if the FDA determines that thirty-day notice is inadequate, it will

continued . . .
sets of device changes, while FDA regulations set out a less rigorous procedure than those applicable to the other three types of PMA supplements and they will probably not be applicable to software changes. Panel-track supplements, 180-day supplements, and real-time supplements require in-depth review and approval by the FDA prior to the change being implemented and marketed. This process may involve a full PMA review, including a review by an outside panel where changes raise new types of safety and effectiveness questions or where there are no accepted methods to evaluate the safety and effectiveness of the changed device.

Panel-track PMA supplements should be filed where there is a significant change in design or performance of the device or a change in the indication for use of the device that requires substantial new clinical data. There is a potential that some software may result in a device able to be used in a different surgical procedure or physiological location and trigger the need for a panel-track PMA supplement. However, it is important to recognize that it wouldn’t necessarily be the software changes alone that trigger the need for a panel-track supplement, but be the changes in indication for use that engages a need for review regardless of whether or not the device software was modified. Furthermore, there is a potential for changes in both the software and hardware such as those required to make wireless devise safer may engage a panel-track PMA supplement.

A 180-day PMA supplement should be filed where the change notify the manufacturer that a 135 day PMA supplement will be required; FDA, Modifications to Devices Subject to Premarket Approval (PMA) – The PMA Supplement Decision, http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm089274.htm (last visited Mar. 29, 2014) (providing that manufacturers should note that even if they fall under a thirty-day notice procedure quality systems regulations require assessment of design changes including risk analysis, verification and validation, and the notice alone will not fulfill all manufacturer obligations).

136 21 C.F.R. §§ 814.39(a), (d), (f).
137 21 C.F.R. § 814.39(c) (“All procedures and actions that apply to an application under § 814.20 also apply to PMA supplements except that the information required in a supplement is limited to that needed to support the change.”); FDA PMA CHANGES, supra note 3.
138 21 U.S.C. § 379i(4)(B); U.S. FOOD & DRUG ADMIN., supra note 129, at 7-8 (providing that panel-track PMA supplements are most appropriate for where new clinical data is required to assure safety and effectiveness of the device where there have been changes in indication for use including changes in the: intended patient population, disease state, or changes in the device use such as duration of use, anatomical site or surgical procedure).
139 U.S. FOOD & DRUG ADMIN., supra note 129, at 7-8 (listing examples of such changes may include changes that result in a smaller or larger emission of energy-current or laser).
does not fall under the definition of a panel track supplement and there has been a significant change in software.\textsuperscript{140} Less clinical data is required for changes falling under the 180-day supplement as compared to a panel-track supplement; the 180-day supplement only requires new preclinical testing or preclinical testing and limited confirmatory clinical data.\textsuperscript{141} Software changes may thus proceed to market via this pathway, and FDA Guidance provides two examples of hardware and software change in devices to which a 180-day PMA supplements were appropriate.\textsuperscript{142}

A real-time PMA supplement is appropriate for a minor change to a device’s design or software, and requires that the applicant request and the agency grant a meeting for joint review and determination of the statute of the supplement.\textsuperscript{143} Applicable changes should be reviewed by a single reviewer with expertise in one scientific area, and there should be a FDA accepted test method, recognized standard or guidance document applicable to the review.\textsuperscript{144} Although the FDA does not further elucidate what types of software modifications it

\begin{footnotes}
\item[140] 21 U.S.C. § 379i(4)(C) (2012) ("[A] significant change in components, materials, design, specification, software, color additives or labeling.").
\item[141] U.S. FOOD & DRUG ADMIN., supra note 129, at 11-12.
\item[142] U.S. FOOD & DRUG ADMIN., supra note 129, at 13. In the first example the manufacturer modified the device’s computer motherboard, operating system and software for the user interface screens. U.S. FOOD & DRUG ADMIN., supra note 129, at 13. The manufacturer and conducted bench testing (including software and functional testing) to demonstrate that the modified device met the original device’s specifications. U.S. FOOD & DRUG ADMIN., supra note 129, at 13. The FDA agreed that clinical data was not needed to evaluate the performance of the modified device because the treatment parameters and algorithm remained the same. U.S. FOOD & DRUG ADMIN., supra note 129, at 13. In the second example, a manufacturer changed the type of battery and the LCD display used in a device requiring changed to the circuit board and software in the device. U.S. FOOD & DRUG ADMIN., supra note 129, at 13. Preclinical testing including electric safety, battery life, software and functionality was required because the changes impacted the electrical characteristics of the device. U.S. FOOD & DRUG ADMIN., supra note 129, at 13. Preclinical testing demonstrated that the modified device operated within the original device’s specifications and the FDA did not require clinical data, and determined that the submission of a 180-day supplement was appropriate. U.S. FOOD & DRUG ADMIN., supra note 129, at 13.
\item[143] U.S.C. § 379i(4)(D)(2012); U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY AND FDA STAFF: REAL-TIME PREMARKET APPROVAL APPLICATION (PMA) SUPPLEMENTS 3-4 (2006), available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089612.pdf (providing that real-time PMA supplements are “appropriate for a minor change that can be expected within a product line, which includes changes to . . . software, instructions for use, warnings, or precautions or other labeling that does not affect the indications or contraindications”).
\item[144] U.S. FOOD & DRUG ADMIN., supra note 129, at 24.
\end{footnotes}
would deem to be minor and thus appropriate for a real-time PMA supplement, it is likely that many software patches that affect the safety and effectiveness of a device and therefore cannot be approved through a periodic report may proceed through the real-time pathway.

Where the change in the device does not affect the safety or effectiveness of the device, the manufacturer’s obligations are less onerous and the FDA may allow the change to be reported in a periodic report or a thirty-day supplement. Periodic reports must identify changes for which a PMA supplement is not required. Where a device change is only required to be noted in a periodic report to the FDA, the manufacturer is permitted to market the changed device prior to its being reported to the FDA. Although the FDA typically requires that changes not affecting safety and effectiveness to be reported in a periodic report, the FDA may provide in the PMA approval order that such changes must be reported in a thirty-day supplement. The FDA acknowledged in its 2005 Guidance document that, if a software patch did not have an adverse effect on the safety and effectiveness of the medical device, it would only need to be reported in a periodic report. It is thus possible for many software changes to proceed through this reporting method; however, manufacturers must be careful to ensure that they correctly assess that the change does not

145 U.S. FOOD & DRUG ADMIN., supra note 129, at 3-4; 21 C.F.R. § 814.39(a), (b).
146 21 C.F.R. §§ 814.82(a), 814.84(b); U.S. FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF: ANNUAL REPORTS FOR APPROVED PREMARKET APPROVAL APPLICATIONS (PMA) 2 (2014), available at http://www.fda.gov/downloads/ MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089398.pdf (providing that PMA approval orders commonly require that a report be submitted one year from the date of approval and annually thereafter; however, the FDA may require more frequent periodic reports).
147 21 C.F.R. §§ 814.39(a), (b); U.S. FOOD & DRUG ADMIN., supra note 146, at 3.
149 21 C.F.R. § 814.39(e)(1)(ii); 21 C.F.R. § 814.39(e)(2) (providing that if the change is required to be reported in a thirty-day supplement, the change may be made thirty days after the FDA files the supplement unless FDA informs the manufacturer otherwise during the thirty-day period); FDA PMA CHANGES, supra note 3 (“FDA may allow certain changes to be reported in an annual report or 30-day supplement an [sic] instead of a PMA supplement submission. (If this method is utilized, FDA will typically request that the information be reported in the annual report and not as a 30-day supplement.”); U.S. FOOD & DRUG ADMIN., supra note 129, at 3 (providing that FDA notes that they have not identified cases for which the thirty-day supplement provision can be effectively applied).
150 U.S. FOOD & DRUG ADMIN., supra note 16, at 5.
have an effect on safety and effectiveness.

Trivial changes do not have to be reported to the FDA at all. It is unlikely that any software changes would ever amount to trivial and therefore the minimum obligation would likely be to report a software change in an annual report or thirty-day supplement.

c. Obligation to Report Corrections

Where a change is made to a legally marketed medical device, a manufacturer must assess its obligation to report the change pursuant to FDA regulations in addition to any quality control, approval (PMA supplement or notice), or clearance requirement. A manufacturer must report to the FDA any corrective change in a device, if the correction was taken to reduce a “risk to health” posed by the device. The reporting obligation is applicable to all types and classifications of devices and applies regardless of whether the correction was needed due to user error. A change in software may thus require reporting where it is taken to reduce a risk to health. The FDA has indicated that cybersecurity patches would not require reporting where they are addressing a cybersecurity vulnerability and not a risk to health.

B. Combination Products

Combination products are therapeutic and diagnostic products that combine drugs, biological products, and/or medical devices. Any software containing combination product will be part medical device, therefore the potential blending options for software containing combination products include: drug/medical device; biologic/medical device; or drug/biologic/medical device.

A combination product involves component parts that would normally be regulated by at least two different FDA Centers each of

---

151 FDA PMA CHANGES, supra note 3 (“Trivial changes, such as changes in the color of a label would not have to be included in the postapproval periodic report.”).
152 See 21 C.F.R. § 806.10 (2013).
153 21 U.S.C. §§ 360i(g) (2012); 21 C.F.R. § 806.10.
155 HHS, supra note 109, at 5.
157 See id.
which follow distinct sets of regulations; in certain circumstances compliance with both centers regulations is not possible.\textsuperscript{159} The OCP was created to address Center conflicts and provide a source of guidance for the regulation of combination products.\textsuperscript{160} All combination products first go through the OCP, which designates a center to address the premarket submission based on the “primary mode of action” of the item.\textsuperscript{161} In most instances, regulation of the entire combination product is performed by one marketing application or submission, however, consultation between centers is permitted and in appropriate cases, the OCP may require separate applications to multiple centers.\textsuperscript{162}

Each FDA Center regulates changes to a legally marketable item in different ways. As described in detail above, the CDRH imposes postmarket quality system regulations and also regulates device modifications in a manner that depends on the impact that the change has as well as whether the device was originally cleared via the 510(k) pathway or approved via a PMA.\textsuperscript{163} Since July 22, 2013, device quality system design controls apply to all combination products that include a device constituent part.\textsuperscript{164} As a result, no matter whether

\textsuperscript{159} See supra text accompanying note 58. With respect to submission requirements for changes, the drugs and biologics regulations are similar, but they differ significantly from the device regulations, see infra text accompanying notes 166-72.


\textsuperscript{161} 21 C.F.R. §§ 3.2(m), 3.4(a), (b); see also Definition of Primary Mode of Action of a Combination Product, 70 Fed. Reg. 49,848, 49,850 (Aug. 25, 2005) (codified at 21 C.F.R. pt. 3) (providing that where a combination product has two independent modes of action, or the most important therapeutic action cannot be determined, the FDA has produced an algorithm to determine the center assignment. The algorithm directs a center assignment based on consistency with other combination products raising similar types of safety and effectiveness questions, or to the center with the most expertise to evaluate the most significant questions raised by the combination product.). See also Intercenter Agreement Between the Center for Drug Evaluation and Research and the Center for Devices and Radiological Health, U.S. FOOD & DRUG ADMIN. (April 4, 2013), http://www.fda.gov/CombinationProducts/JurisdictionalInformation/ucm121177.htm (granting certain combination products to one center for market approval, with interagency consultation being required in specified circumstances).


\textsuperscript{163} See supra notes 114, 118-19, 123-25, 129-54 and accompanying texts.

\textsuperscript{164} Current Good Manufacturing Practice Requirements for Combination continued \ldots
CDER or CDRH is responsible for regulating changes made to a combination product (containing a drug and device component), the manufacturer will nevertheless be required to test, verify, and validate all changes made to the combination product’s components pursuant to the device design control regulation.\textsuperscript{165} Therefore, software verification and validation will be required to be performed for all software changes regardless of what center is responsible for the specific combination product.

When a change is made to a licensed drug, there are multiple routes through which the changed drug may proceed to the market depending on whether the changes have a substantial, moderate, or minimal potential to have “an adverse effect of the change on the identity, strength, quality, purity, or potency of the product as they may relate to the safety or effectiveness of the product.”\textsuperscript{166} Changes with a “substantial potential” to have an adverse effect are termed major changes and require submission and approval of a “Prior Approval Supplement.”\textsuperscript{167} Moreover, changes with a “minimal potential” to have an adverse effect need only be reported in an annual report to the FDA.\textsuperscript{168} There are two types of supplements that may be filed for changes with a “moderate potential” to have an adverse effect. The two types of supplements for moderate changes include: “Supplement–Changes Being Effected in 30 Days” wherein the drug product can be distributed thirty days after the FDA receives the supplement, unless the applicant is informed otherwise within the thirty days,\textsuperscript{169} and “Supplement–Changes Being Effected” for changes specifically identified by the FDA.\textsuperscript{170} Although drugs with moderate changes may be distributed prior to review (after thirty days or right away depending on the supplement type), the FDA may order the manufacturer to cease distribution if the FDA disapproves of the

\textsuperscript{165} Id. at 4,315 (providing that all components of the combination product and not just the device component are subject to the device design controls in 21 C.F.R. § 820.30).


\textsuperscript{167} 21 C.F.R. § 314.70(b) (2013).

\textsuperscript{168} 21 C.F.R. § 314.70(d).

\textsuperscript{169} 21 C.F.R. §§ 314.70(c)(3), (5).

\textsuperscript{170} 21 C.F.R. § 314.70(c)(6).
change in a subsequent review.\textsuperscript{171}

The pathways through which a changed biologic may proceed to market are similar to drugs and depend on whether the change has a substantial, moderate, or minimal potential to “adversely affect the identity, strength, quality, purity, or potency of the drug as they may relate to the safety or effectiveness of the drug.”\textsuperscript{172}

It may be argued that a common sense approach would be for a modification to a combination product to be regulated based on the component of the combination product being modified.\textsuperscript{173} However, the industry custom is for the center that was originally assigned review responsibility for the premarket submission or approval to retain such review responsibility for changes and may consult with other centers.\textsuperscript{174} This approach is echoed in the OCP’s 2013 Draft

\textsuperscript{171} 21 C.F.R. § 314.70(c)(7).

\textsuperscript{172} 21 U.S.C. § 356(a) (2012); 21 C.F.R. §§ 314.70, 601.12(b)-(d) (providing that changes with a “substantial potential” to have an adverse effect require approval of a supplement prior to distribution of the changed product whereas changes resulting in a “moderate potential” of an adverse effect do not require approval, all that is required is for the applicant to submit a supplement thirty days prior to distributing the changed product. Moreover, changes with a “minimal potential” to have an adverse effect need only be reported in an annual report to the FDA); see also FDA, GUIDANCE FOR INDUSTRY: CHANGES TO AN APPROVED NDA OR ANDA 3 (2004), available at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm077097.pdf.

\textsuperscript{173} Following this logic, a modification to a drug component would be regulated by the CDER, a modification to a biologic governed by CBER regulation and a modification to a device (including software) governed by the CDRH.

\textsuperscript{174} The FDA has permitted software modification to a PMA approved device with a combination product component to proceed through the device regulatory framework requiring a PMA supplement, modification to the software of a device approved through a PMA application and a subsequent supplement added a drug coated lead resulting in a combination product. See Premarket Approval (PMA) Database PMA Number P030054 S009, FDA, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpm a/pma.cfm?id=17667 (last visited Mar. 29, 2014) (providing that original PMA approval order for “Dual Chamber Implantable Cardiovascular Defibrillator With Biventricular Pacing”); Premarket Approval (PMA) Database PMA Number P030054 S130, FDA, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpm a/pma.cfm?id=17564 (last visited Mar. 29, 2014) (providing that supplement approved for the addition of a “drug eluding permanent left ventricular pacemaker electrode” resulted in product being classified as a combination product); Final Review Memorandum from the Food and Drug Admin Regarding PMA Number P030054 S130 (May 6, 2010), available at http://www.accessdata.fda.gov/cdrh_docs/pdf3/P030054S130M.pdf (providing drug being added to device to result in combination product was the same as that approved for a similar lead, and a condition of approval of the supplement was compliance with the same postapproval conditions as the other product. “The agreement and condition of approval text was reviewed and found acceptable by CDER.”); Premarket Approval (PMA) Database PMA Number P030054 Supplement S223, FDA, http://www.accessdata.fda.gov continued . . .
Guidance, providing that changes to the combination product are required to be submitted to the center with original jurisdiction over the combination product, in the form of supplement, notice or report required by that center.\textsuperscript{175} The Draft Guidance proposes a process for determining what type of submission to make for a change to a combination product approved under a PMA, New Drug Application (NDA) or Biologics License Application (BLA) based on what part of the combination product is being modified and what type of supplement would be required if the changed component were a standing-alone device.\textsuperscript{176} For example, consider an insulin pump containing a novel insulin-like drug that was approved as a combination product through a NDA by the CDER, which contained software that was subsequently modified. In order to determine what type of supplement would have to be changed for the software modification one needs to consider what type of supplement would need to be filed if the changed portion of the combination product (in this case the device) were a stand-alone device. The Guidelines then provide a table in which one correlates the type of standing-alone supplement under device regulations with type of supplement would be required under the combinations approved center, CDER.

\textsuperscript{175} For example, a software modification to a drug-device combination product originally approved through a NDA by the CDRH would require a Prior Approval Supplement, or Annual Report complying the content requirements for changes to Drugs. \textit{See U.S. FOOD \& DRUG ADMIN., supra} note 162, at 4.

\textsuperscript{176} \textit{U.S. FOOD \& DRUG ADMIN., supra} note 162, at 4, 6 (providing that, first, identify the type of application used to obtain approval of the combination product (PMA, NDA, BLA). Second, consider what part of the combination product has changed, and what type of approval would be required if the changed part were a stand-alone device (for example, a software change would involve a change to the device component and if the device were PMA approved the change might require either a PMA 180 day supplement, a PMA Real-Time Supplement or a thirty-day notice). Third, if approval of the combination product was through the same Center as the changed part, submit the postapproval submission from the Second Step. If the changed part is different than the original center (such as where a drug/device combination product was originally approved by the CDER, and a software change has been made), use the table provided in the Guidance to identify what type of submission should be made. Guidance Table 1 pertains to changes made to the device component of a combination product where the original approval was made under a NDA or BLA, and will thus apply to software changes where the combination product was not originally approved under device regulations. Table 1 provides a correlation between the type of submission that would have been required under the device regulation if the changed part were a standalone device and what type of submission is required under the biologics or drug regulations).
III. EXAMPLES AND APPLICATION

A. Updating Commercial Off the Counter Software to Prevent Malware Infection

Many manufacturers of medical devices are reluctant to issue or permit the installation of security updates (including security patches and anti virus software) for COTS software running on their legally marketed medical devices.\(^{177}\) One of the reasons given for this reluctance is concern over whether such modifications impose obligations under FDA regulations.\(^{178}\) As discussed in Part II of this article, the specific obligations a manufacturer will face when modifying a legally marketable device depends primarily on the effect of the change as well as the method through which the device was originally cleared or approved for market.\(^{179}\) There are three potential sources of obligations a manufacturer faces for change: quality system obligations,\(^{180}\) reporting obligations,\(^{181}\) and clearance or approval obligations.\(^{182}\)

The most onerous source of obligations for manufacturers in response to adding COTS software security updates is design verification and validation requirements imposed under FDA’s quality system regulations. Quality system regulations require that manufacturers establish and implement design controls wherein the manufacturer verifies, validates, and records any design changes.\(^{183}\) Any software change, including the addition of COTS software security updates, will require the manufacturer to verify the code through code inspection, and testing of input and output, as well as to conduct risk analysis and validate the changed software in its actual or

---

\(^{177}\) INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 9 (“Mr. D'Souza indicated that GAO had talked with some manufacturers about the patching issue and manufacturers indicated they did not want to patch devices to jeopardize their certification. Mr. D'Souza indicated that the general feedback was that the possible benefit of issuing a patch is far outweighed by the risk – the issue is one of liability.”).


\(^{179}\) See supra Part II.A.2.b

\(^{180}\) See supra Part II.A.2.a

\(^{181}\) See supra Part II.A.2.c

\(^{182}\) See supra Part II.A.2.b

simulated use environment. There are valid reasons for requiring manufacturers to verify and validate that their devices will continue to operate as specified after security updates are added, as updates can cause problems themselves. It is not uncommon for anti-virus software updates to cause problems; in 2010 numerous hospitals and universities were negatively affected by a malfunctioning McAfee anti-virus update that impaired their ability to provide care. The update resulted in the anti-virus software misclassifying a normal Windows file as a virus, causing any computers that had installed the update to enter into a continuous reboot cycle. If a security update like the defective McAfee update had been installed on a computer running a medical device without prior quality system controls over how the update would affect the device, the device could be rendered nonfunctional and potentially could have caused serious harm.

FDA reporting obligations require that any corrective change taken to “reduce a risk to health” be reported to the FDA. In its 2005 Guidance, the FDA indicates that patches designed to address cybersecurity vulnerability would not require such reporting as they are implemented to address cybersecurity vulnerability, not a risk to health. Therefore, there are no reporting obligations for updating virus scanning software or security patches.

A manufacturer’s obligation to re-submit for 510(k) clearance or file a PMA supplement largely depends on whether the modification may significantly affect the safety or effectiveness of the device. Where there is an effect on the safety or effectiveness of the device, new 510(k) clearance or the filing of a PMA supplement is generally

---

186 Fu, supra note 6, at 99; Tobin, supra note 185; Svensson, supra note 185.
187 21 U.S.C. § 360i(g); 21 C.F.R. § 806.10.
188 U.S. FOOD & DRUG ADMIN., supra note 109, at 5.
189 Although the manufacturer will have no reporting obligations under 21 C.F.R. § 806, the manufacturer of a PMA approved device may nevertheless have an obligation to notify the change in an annual report. See supra notes 144-52 and accompanying text.
190 See supra notes 115-16, 131-32 and accompanying text.
A software update adding a security patch or anti-virus software will be unlikely to affect the safety and effectiveness of the device, it merely addresses cybersecurity vulnerability and permits the device to operate as originally intended. As a result, a manufacturer will not have an obligation to obtain a new 510(k) clearance for updating a virus scan or security patch where the device was originally cleared through the 510(k) pathway. However, where the device was originally approved for market through PMA, the manufacturer must notify a change in a virus scanning software or security patch in the manufacturer’s periodic report, but need not file a PMA supplement.

Therefore, a manufacturer does not, in any circumstance, require permission from the FDA to update COTS software when adding or updating a software patch or anti-virus software. However, prior to issuing an update, the manufacturer must comply with quality system design controls and verify and validate that the updates do not alter the proper functioning of the medical device. These design control requirements prevent the manufacturer from permitting users to install any update that becomes available from a COTS software retailer without the medical device manufacturer conducting additional testing. Such testing will undoubtedly cost money and take time, resulting in device manufacturers not being able to be as responsive to security threats as producers of non-medical device software.

Users have asked the FDA to clarify to manufacturers that they need not re-obtain 510(k) clearance for a device when they permit the addition of a COTS security update. It would therefore be beneficial for the FDA to clarify the obligations stated above with respect to security patches and virus scanning software, and that the mere fact that a manufacturer is not required to re-obtain 510(k) clearance or file a PMA supplement is not the end of the manufacturer’s obligations. Therefore, even if the FDA were to clarify the specific point requested by users, it would not necessarily result in more manufacturers permitting such software updates to be installed on their devices due to the fact that the manufacturers still have verification and validation requirements before approving and issuing such updates.

191 See supra notes 115-16, 131-32 and accompanying text.
192 See supra text accompanying notes 115-16.
193 See supra text accompanying notes 130-31.
195 INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 9.
A manufacturer’s obligations upon issuing a security update are separate from the question of whether a manufacturer must issue such updates. The issue can be reduced to the question of whether manufacturers have an obligation to ensure that their devices are safe from malware and thus continue to run smoothly, and if manufacturers have such an obligation, what is the extent of this obligation.

Manufacturers are responsible for ensuring that their medical device performs according to specifications. However, other than the quality systems regulations requiring design controls and risk analysis, there are no explicit regulations requiring a device manufacturer take cybersecurity risks into effect when evaluating the design of its devices. In its May 2005 Guidance, the FDA recommended that manufacturers take the environment in which the device would be working into account in its quality systems risk analysis. This Guidance specifically states:

Software applications designed to protect information systems, including Software Devices, from harmful or malicious code (“viruses,” “worms,” etc.) are becoming more commonplace as devices become increasingly interconnected and therefore exposed to the external information environment . . . We recommend that your software design should take into account both the capabilities and liabilities of the interfaces provided with your device, and in particular that your hazard analysis and mitigations encompass these issues.\(^{196}\)

On its face this Guidance seems to require that manufacturers have some sort of obligation to take cybersecurity threats into account and to actively permit security patches and antivirus software to be updated to protect against such threats. However, there are many reasons that support the 2005 Guidance not to be interpreted as imposing such obligations. First, the Guidance is not binding and does not form any legal obligations.\(^{197}\) Second, FDA Deputy Director of the Division of Electrical and Software Engineering, Brian Fitzgerald, recently indicated in statements to the Information Security and Privacy Advisory Board that although “it is not FDA policy to prevent patching of devices . . . that it is important for knowledgeable customers in the security field to be involved in the procurement processes for medical devices.”\(^{198}\) This statement intimates that the FDA is taking a sort of buyer-beware attitude, where some of the onus

\(^{196}\) U.S. FOOD & DRUG ADMIN., supra note 16, at 18.
\(^{197}\) U.S. FOOD & DRUG ADMIN., supra note 16, at 1.
\(^{198}\) INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 9.
is on the purchaser to obtain products that meet its security needs.

Third, a manufacturer may reasonably conclude after conducting a risk analysis, as part of their quality systems obligations, that the appropriate action to mitigate risk is that the device is run in a security environment behind a firewall.\footnote{INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 8.} If a firewall was found to be a sufficient way to reduce risk, mandatory security updates would not be necessary. Furthermore, if a manufacturer provides a functioning device with instructions that suggest customers use a firewall, security problems (i.e. malware infection) that arise in the device from the user’s subsequent networking, or from the device itself, cannot be attributed to the manufacturer.\footnote{In order for a manufacturer to rely on this argument, the manufacturer may have to notify the users of what sort of security protections (firewalls) they should take to keep their devices safe.} The sole fact that protecting all of their devices behind firewalls is expensive for medical centers does not preclude this as a viable option.

Fourth, requiring manufacturers to use commercially available security patches and anti-virus software to protect their devices against malware may be problematic as it does not take into account that many devices run on customized operating systems for which there are no compatible commercially available updates.\footnote{Wirth, supra note 7, at 27; INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 8.} Furthermore, the lifespan of medical devices is often longer than the lifespan of the COTS operating systems that they are based on.\footnote{INFO. SEC. & PRIVACY ADVISORY BD., supra note 19, at 8; FAQs for End of Windows XP Support, MICROSOFT, http://www.microsoft.com/en-us/windows/endofsupport.aspx (last visited Mar. 29, 2014) (stating that support for Windows XP will end on April 8, 2014).} Even if commercially available patches would function with a particular device, it is likely that during the lifespan of these devices security patches will stop updating for the devices’ operating system.\footnote{Wirth, supra note 7, at 28 (“Driven by cost and design restrictions, available memory space is often limited. This has led many manufacturers to use customized or scaled-back versions of standard operating systems. From a design perspective this is a perfectly reasonable approach; however, as a result, it becomes difficult to apply software patches or to utilize common security software solutions”).} Using an operating system for which updated patches are not available would cause a huge risk because any security vulnerabilities in the system may become widely known by people with nefarious intent and exploited.

While the imposition of a duty on device manufacturers to protect their devices from cybersecurity threats by mandating the use of commercially available security patches and anti-virus software
sounds overwhelming, such a burden would be magnified by a mandate that required device manufacturers to take additional actions to protect their systems against cybersecurity vulnerabilities where there are no commercially available solutions. It is important to consider what actions the manufacturers should be required to take to protect their devices if no commercially available solutions exist. One option is that the manufacturers would have to obtain or create the equivalent of commercially available patches. Another option is to require manufacturers to update their devices to run on systems with commercially available security updates. An additional option would be for the manufacturers to use other security options such as a firewall, or to stop using commercially available, off-the-counter software in their devices. It is unlikely that a manufacturer would be able to sustain producing security patches comparable to those produced by a large company. Furthermore, shifting the device to a different operating system may require extensive work, affect the safety and efficiency of the device and consequently require the submission of new clearance or PMA supplements. However, if the use of a firewall were found to be appropriate in such cases, it would seem reasonable for a firewall to be used as a protective measure throughout a device’s lifespan and this would be a complete solution to the problem. Nevertheless, if the FDA determined that a firewall was not appropriate, such obligations might push the device industry to stop using commercially available off-the-counter software and use more secure proprietary critical systems designs, such as those used in avionics. Such an approach would be consistent with the recommendation of computer software engineers and is likely to reduce the risk of cybersecurity threats.

The FDA should address and clarify several issues that have arisen with respect to security updates for COTS software running on medical devices. First, the FDA should clarify that such security updates do not require that the manufacturer obtain FDA permission, but that nevertheless the manufacturer must comply with design controls and verify and validate the device in the presence of the security update. The design control obligations make it clear that users are not permitted to install such updates unless directed to by the

---

204 An upgrade to a new operating system may require major changes in other software elements and thus may require a significantly different testing scheme to validate the changes. See U.S. FOOD & DRUG ADMIN., supra note 109, at 4-5. Such a change would potentially raise new issues of safety and effectiveness. See U.S. FOOD & DRUG ADMIN., supra note 109, at 4-5.

205 Fu, supra note 6, at 105.

206 Fu, supra note 6, at 105.
manufacturers. Second, the FDA should clarify a manufacturer’s obligations to keep its device functioning as intended, in light of the knowledge that many device computers are laden with malware that affect their work. Specifically, whether there is an obligation on the user to keep the device free of malware through the use of firewalls, or whether the manufacturer is under an obligation to test and issue commercially available software updates, or create and issue its own security updates.

B. Updating software on stand alone medical devices in response to security threats

When it comes to issuing updates for proprietary device software, there does not seem to be the same level of manufacturer resistance or confusion as there is with updating COTS software. This is potentially due to the fact that manufacturers have a higher motivation to make software modifications that fix problems or add features that directly impact the functioning of their own products. Since there is no evidence of complaints from users or manufacturers regarding when modifications require FDA involvement the only benefit of the FDA clarifying such obligations would be to streamline its workload by ensuring that modifications that could be submitted through procedures that require less FDA involvement actually progress through those pathways.207

As discussed above, major sources of concern in the medical device industry are the privacy and security vulnerabilities facing medical devices, and in particular, facing wireless medical devices such as automated external defibrillators (AEDs), insulin pumps, and pacemakers.208 These devices are susceptible to malware and hacking due to vulnerabilities in their software, such as the execution of unintended code, flaws in password protection, and faulty software

207 For example, a special 510(k) submission requires less paperwork than a traditional 510(k) submission. Different PMA supplements also require varying levels of work for the manufacturers and therefore differing levels of FDA involvement.

updating and communication mechanisms.\textsuperscript{209} Software that permits unintended codes to be executed is susceptible to malware becoming installed on the system, and once installed, could potentially transfer wirelessly to other devices.\textsuperscript{210} The ability of a medical device to wirelessly receive downloads creates a portal for software contamination and security breaches if not secured properly.\textsuperscript{211} Additionally, if malware were to infect a device it could potentially interfere with the functioning of the device or obtain private data.\textsuperscript{212} Passwords for medical devices need to be securely protected, otherwise outsiders could gain access to the device and alter its function or obtain personal data.\textsuperscript{213} Wireless medical devices were originally thought to be relatively safe and therefore there was little incentive for manufacturers to add security features.\textsuperscript{214} Although a complete redesign of these systems may be ideal, it is likely that fixes to the devices will proceed via software and potentially hardware changes to the devices. Computer software engineers have suggested that the most effective way to control the spread of malware on medical devices is to strengthen their software.\textsuperscript{215}

The three sources of potential obligations for manufacturers where changes are made to software are the same as described in part III.A of this article, namely: quality system obligations,\textsuperscript{216} reporting obligations,\textsuperscript{217} and clearance or approval obligations.\textsuperscript{218} Quality system obligations and reporting obligations are the same as described above, with the caveat that changes to propriety software may be made to reduce a risk to health and thus unlike COTS security updates may engage the manufacturers’ obligation to report the change to the FDA.\textsuperscript{219}

Compared to COTS security updates, the range of software

\textsuperscript{209} Hanna et al., supra note 208; Clark & Fu, supra note 26, at 3; U.S. GOV’T ACCOUNTABILITY OFFICE, supra note 208, at 15 (intentional threats to implantable medical devices include unauthorized access, malware, and denial of service attack).

\textsuperscript{210} Hanna et al., supra note 208, at 4.

\textsuperscript{211} Maisel & Kohno, supra note 208, at 1165.

\textsuperscript{212} Hanna et al., supra note 208, at 4.

\textsuperscript{213} Hanna et al., supra note 208, at 4.

\textsuperscript{214} See Wayne Burleson et al., Design Challenges for Secure Implantable Medical Devices, 2012 PROC. DESIGN AUTOMATION CONF. 12, available at https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf (explaining that traditionally bug-adverse manufacturers had little incentives to add security mechanisms that might slow regulatory approval or cause problems).

\textsuperscript{215} Id.

\textsuperscript{216} See supra Part II.A.2.a.

\textsuperscript{217} See supra Part II.A.2.c.

\textsuperscript{218} See supra Part II.A.2.b.

\textsuperscript{219} 21 C.F.R. § 806 (2013).
updates for proprietary device software is likely to be more diverse and thus have the potential to require a variety of types of PMA supplements or 510(k) clearance submissions. A major factor as to what type of action is required for a software modification is whether the update affects the safety or effectiveness of the device.\textsuperscript{220} Where there has been an effect on the safety or effectiveness of the device, new 510(k) clearance or the filing of a PMA Supplement is generally required.\textsuperscript{221} The need for a significantly different testing scheme to validate the software changes supports that there has been a change in the safety and effectiveness of the device.\textsuperscript{222} Manufacturers have been filing PMA supplements for software changes in medical devices.\textsuperscript{223}

\textsuperscript{220} See supra notes 115-16, 131-32 and accompanying text.
\textsuperscript{221} See supra notes 115-16, 131-32 and accompanying text.
\textsuperscript{222} FDA 510(k) CHANGES, supra note 3, at 15-16.
\textsuperscript{223} PMA supplements have been filed for modifications to device and testing software including: new versions of software, adding functions to software including modifications to support new device components; see PMA Database: Itrel® Totally Implantable Spinal Cord Stimulation System, PMA Number P840001, FDA, available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=3665 (last visited Mar. 29, 2014) (25 of 218 supplements filed for the device up until Apr. 19, 2013 expressly stated in their descriptions that they involved modifications to device software or testing software. Numbers for supplements involving software include: S022, S038, S039, S061, S088, S093, S098, S156, S168, S171, S172, S173, S186, S189, S190, S194, S196, S200, S201, S216, S222, S227, S230, S231, S233); PMA Database: Medtronic Minimed Continuous Glucose Monitoring System, PMA Number P980022, FDA, available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=15014 (last visited Mar. 29, 2014) (25 of the 117 PMA supplements filed for the device from 2000 to Apr. 6, 2013 expressly stated in their descriptions that they involved modification to device software. Numbers for supplements involving software include: S007; S020; S023; S024; S028; S031; S033; S034; S037; S043; S047; S052; S071; S073; S080; S081; S085; S092; S099; S104; S107; S112; S117; S123; S124); PMA Database: Clarion Multi-Strategy Cochlear Implant, PMA Number P960058, FDA, available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=14154 (last visited Mar. 29, 2014) (9 of 73 supplements filed for the device up until Apr. 19, 2013 expressly stated in their descriptions that they involved software. Numbers for the supplements involving software include: S010, S011, S022, S029, S049, S082, S085, S089, S093); For devices containing a wireless component, approval has been obtained for both changes to software on the implantable device itself as well as the proprietary network based software that resides on a computer server connected to the internet, see PMA Database: Medtronic Minimed Continuous Glucose Monitoring System, PMA Number P980022, Supplement Number S033, FDA (Aug. 24, 2008), available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=7601 (last visited Mar. 29, 2014) (changes to computer based software included “Approval for a change to the carelink personal therapy management software for diabetes (mmt-7333) the carelink personal therapy management software for diabetes is a network based software system residing on a computer server platform connected to the internet. The purpose of this system is to take information transmitted from insulin continued . . .
Even though one only need file a PMA supplement where there has been an effect on the safety or effectiveness of the device, one cannot draw an inference that software updates for which PMA supplements were filed actually had such a change as it is unknown whether it was the manufacturer who chose to file a PMA supplement, or if the FDA required its filing. In any event, it is likely that many of the changes to address vulnerabilities in wireless devices will affect the safety and effectiveness of the device.

Where there is a change that affects the safety and effectiveness of a 510(k) cleared device, the modified device may be cleared for marketing through traditional 510(k) clearance or the less onerous special 510(k) clearance. It is likely that many software changes will be able to proceed via special 510(k) clearance wherein the manufacturer need only provide details about the changed software element and not the whole device. Moreover, the FDA’s 510(k) Premarket Notification Database contains examples of software changes to 510(k) cleared devices where in the modification proceeds to market via a special 510(k) submission.224

pumps, continuous glucose monitors and glucose meters, and logbook data entered by the patient, and turn it into medtronic carelink therapy management software for diabetes reports. The reports provide information that can be used to identify trends and track daily activities; such as carbohydrates eaten, meal time, insulin delivery, and blood glucose readings. The software version 4.6 is a revision to implement several feature enhancements, which include a logbook diary report, removal of Roche accu-check ‘aviva’ and compact plus meters from meter listings displayed for users located in countries other than U.S. and Canada, and consolidation of the help system that serves as instructions for use.”); PMA Database: Medtronic Minimed Continuous Glucose Monitoring System, PMA Number P980022, Supplement Number S047, FDA, (Apr. 6, 2009), available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=20175 (last visited Mar. 29, 2014) (changes to fix software glitches on the devices described as “Approval for a modification to the solutions software for the cgmss ipro continuous glucose recorder (mmt-7319) to add an auto detect feature to allow the software to automatically recognize the computer’s active ports and to correct previously identified anomalies”); PMA Database: Medtronic Minimed Continuous Glucose Monitoring System, PMA Number P980022, Supplement Number S112, FDA (Apr. 27, 2012), available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=18709 (last visited Mar. 29, 2014) (“Approval for software modifications (version 2.5a) and related labeling modifications for the paradigm real-time revel pump (models mmt-532, mmt-723, mmt-523k, mmt723k). The paradigm revel insulin pump is a component of the paradigm real-time revel system”).

Where there is a change to a PMA approved medical device affecting the safety and effectiveness of the device, the modified device may be approved for marketing via the filing of a PMA supplement. As discussed in Part II.A.2.b.ii there are multiple types of PMA supplements. Special PMA supplements are applicable where new quality controls have been added to enhance the safety of the device. Therefore, software updates to the devices software itself are unlikely to qualify for a special PMA supplement. Furthermore, thirty-day notice is not applicable to changes in the devices software, as thirty-day notice only applies to manufacturing changes.

The types of PMA supplements that may be applicable to software changes include panel-track, real-time and 180-day PMA supplements. It will likely be rare for a software change alone to engage the need for a panel track PMA supplement. Some security solutions for wireless devices such as the addition of some protective mechanism (requiring a change in hardware and software) to prevent the device from receiving unauthorized communications might require new clinical data and thus require a panel-track PMA supplement.

Significant changes in software that do not require extensive clinical data may proceed through a 180-day PMA supplement, and devices with modified software have proceeded to market in this manner. Minor changes to software that are reviewable by an expert in a single area may proceed via a real-time supplement. Most of the supplements for software changes in the FDA’s PMA database proceed via Real-Time or 180-day PMA Supplements, suggesting that they only involve minor changes or require preclinical data and limited clinical data.

wireless communication system including software modifications, manufacturer conducted software verification and validation testing to confirm that the modified accessory performed as intended and that changes made to the software had no impact on the functionality of the system).

225 21 C.F.R. § 814.39(d)(2) (stating which permissible changes may proceed via special PMA supplement, including: “changes in quality controls or other manufacturing process that add a new specification or test method, or otherwise provide additional assurance of purity, identity, strength, or reliability of the device”).


227 See supra text accompanying notes 138-39.

228 Burleson et al., supra note 214, at 4 (explaining that vulnerabilities could be mitigated by ultrasonic distance bounding, or body coupled communication that would require new device hardware be added).

229 21 U.S.C. § 379i(4)(C) (2012); see also notes 141-42 and accompanying text.

230 U.S. FOOD & DRUG ADMIN., supra note 143.

231 See generally PMA Database: Continuous Glucose Monitoring System, PMA Number P980022, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/continued...
Many modifications to wireless devices addressing security or privacy issues are likely to raise issues of safety and efficacy and will require either a new 510(k) clearance submission or the filing of a PMA supplement. While there is room for the FDA to clarify many points in this area, there is not a large outcry from the public or manufacturers. Thus clarification would largely be to streamline the forms of submissions and supplements required and potentially reduce the workload for the manufacturers as well as the FDA itself. Specifically, it would be useful for more clearance on precisely what types of software changes may precede via special 510(k) clearance, as well as what is a minor change that would permit the filing of a real-time PMA supplement.

C. Updating mobile application medical devices in response to operating system changes.

The FDA’s Guidance on Mobile Medical Applications provides that regulated apps will be subject to 510(k) clearance and PMA, where applicable, as well as general controls. Thus manufacturers (also referred to as developers) of mobile medical apps will be subject to the same types of regulations for software updates already referred to in this article, namely: quality system obligations, reporting obligations, and clearance or approval obligations. While the Guidance advises manufacturers on what sorts of changes to correct problems to an app require reporting to the FDA, the Guidance does not address what sorts of changes require a new 510(k) clearance or a PMA supplement. However, some information can be gleaned from a statement made by FDA CDRH Office of Device Evaluation Director Christy Foreman to the House Energy and Commerce Subcommittee on Oversight and Investigations during a hearing on March 21, 2013 that the “FDA’s proposed mobile medical apps policy would not require mobile medical app developers to seek Agency re-

pma.cfm?id=15014 (last visited Mar. 29, 2014) (of the PMA 25 supplement involving software filed for Medtronic Minimed Continuous Glucose Monitoring System, 17 involved a real-time supplement including S024, S028, S033, S043, S047, S052, S073, S080, S081, S086, S092, S099, S107, S122, S117, S123, S124 and eight involved a 180 day PMA supplement including S007, S020, S023, S031, S034, S037, S071, S104).

232 U.S. FOOD & DRUG ADMIN., supra note 31, at 33.

233 See supra Part II.A.2.a.

234 See supra Part II.A.2.c.

235 See supra Part II.A.2.b.

236 U.S. FOOD & DRUG ADMIN., supra note 31, at 35-36.
evaluation for minor, iterative product changes."\textsuperscript{237} Although this statement was not repeated in the finalized Guidance, this statement coincides with the FDA's approach of not requiring FDA involvement for device changes that do not have an effect on the safety or efficacy of the device.\textsuperscript{238}

It is unclear as to whether mobile medical applications are cleared for specific versions of operating systems in the same way that a medical device may be cleared or approved for use with an operating system such as Windows XP. If it is the intent of the FDA that minor iterative product changes, that do not require FDA permission, include updating of the operating system on which the app runs, the FDA needs to make that clear.\textsuperscript{239} Otherwise, the app manufacturer would be responsible for ensuring that the app only works on a specific operating system version. The impact of updates on mobile medical apps must also be considered in terms of the relative newness of the technology. The Apple App Store opened in July of 2008 and ran apps on the Apple iPhone operating the operating system iOS 2.0.\textsuperscript{240} Although the newest iPhone, the 5s, currently operates on iOS 7,\textsuperscript{241} the changes made through iOS 6 were relatively iterative in nature.\textsuperscript{242} This is in contrast to major changes, such as the roll out of an overhauled platform, seen in the Windows 95 to 98 change.

Quality system requirements including verification and validation testing, in response to mobile platform operating system upgrades, will present unique challenges to manufacturers. For example, when Apple plans to introduce an update for the operating system for one of its mobile devices it notifies app manufacturers of the changes and grants them a limited amount of time to test their apps with a simulator.
that simulates the operating system changes. However, app developers do not have the opportunity to test their own apps on the fully upgraded operating system until Apple has released it. This puts device manufacturers in the position where a user may upgrade the operating system on their mobile platform and continue to use a mobile medical app that has not been verified and validated for use on the upgraded operating system. The limited testing time may become increasingly important in situations where the upgrade is significant and results in the safety and effectiveness of the device being affected, thus requiring FDA involvement. The potential for use of an untested app raises questions including whether manufacturers must ensure that apps will not work on upgraded operating systems without their approval as well as whether manufacturers must notify users about operating system upgrades and that their app is untested on the upgraded operating system, and how such notification would occur.

Many apps are currently approved not only for specific operating system versions but also for specific platforms. For example, the AliveCor App is approved for use with the iPhone 4/4S and 5, and the iBGStar Glucose Monitor is approved for use with the iPhone 5s and earlier models. There are many reasons why an app should only be approved for a specific platform particularly when it relies on a physical element of the platform such as the size of the phone or specific camera included on a particular platform. A change in a

---


245 Some of these questions have been asked by persons in the industry, see Letter from Michael C. Morton, Senior Dir. Global Regulatory Affairs, Medtronic, to Div. of Dockets Mgmt., FDA (Oct. 19, 2011), available at http://www.regulations.gov/#/documentDetail;D=FDA-2011-D-0530-0070 (“Should the distributor play a role in informing app users and manufacturers of a pending operating system change? While the document focuses on the app itself, Medtronic would encourage the FDA to provide guidance on the pathway for postmarket change in both the app and mobile platform operating system. Such guidance might address advance notice by the distributors in the foreseeable event of validation update.”).

246 *FDA Premarket Notification Database*, supra note 39 (AliveCor Heart Monitor is cleared for use with the iPhone 4 or 4S).


248 *FDA Premarket Notification Database*, supra note 39 (AliveCor Heart Monitor continued...
traditional app, such as a camera, or even an adapter would likely constitute a change that would affect the safety and effectiveness of the device and would require FDA involvement. In order to maintain consistency between traditional medical devices and mobile medical apps, the change of the platform should also be analyzed to determine if FDA involvement is required to approve or clear the change. Additionally, it is currently unclear whether a manufacturer has any obligations to prevent a user from using an app on a newer and potentially unapproved platform beyond notifying the user that the device has only been cleared or approved for a specific iPhone version.249

Since the FDA has chosen not to exercise jurisdiction over manufacturers of mobile platforms (such Apple or Toshiba), or distributors of apps (such as the Apple App Store or Android Market), the burden of complying with the FDA’s regulations is solely on the manufacturer of the app.250 Moreover, not only will the manufacturer have the burden of complying with FDA regulations, but they will also be responsible for complying with rules created by the distributors in order to offer the app in the distributors’ stores. Guidance will be required from the FDA for how manufactures should act in situations where they cannot comply with both the distributors’ rules and FDA regulations.

Any FDA limits on a developer’s ability to update their mobile medical app to comply with new operating systems or platforms may place the manufacturer in a situation where it faces conflicting requirements from the FDA and Apple, and thus interfere with the ability of the manufacturer to fix bugs/problems with their app.251

Monitor is a phone case and relies on the dimensions of the iPhone); FDA Premarket Notification Database, PanOptic iExaminer K121405, FDA (Dec. 11, 2012), available at http://www.accessdata.fda.gov/cdrh_docs/pdf12/K121405.pdf (device uses camera on iPhone, designed for iPhone 4 and 4S).

249 An industry participant has requested further FDA guidance on how to display which versions of apps have been approved, cleared or validated, see Letter from Brian E. Harvey, Vice President U.S. Regulatory Policy, Sanofi-aventis, to Div. of Dockets Mgmt., FDA (Oct. 19, 2011), available at http://www.regulations.gov/#!documentDetail;D=FDA-2011-D-0530-0062 (“The second comment is related to the life cycle of the mobile platform and mobile applications. It is a characteristic of these evolving technologies that changes are developed and made available very rapidly. It would be useful to be clear on which version has been verified and validated to obtain clearance/approval from Authorities dependent on the device class.”).


251 Industry participants have requested further guidance on bug reporting and corrections, see Letter from Triangle PEERS, to Div. of Dockets Mgmt., FDA (Oct. 18, 2011), available at http://www.regulations.gov/#!documentDetail;D=FDA-2011-continued...
the case of mobile medical apps running on Apple platforms, changes to an app (including bug fixes) are made as updates through the Apple App Store.\footnote{\textit{App Store Distribution}, \textsc{Apple Developer}, \url{https://developer.apple.com/support/appstore/} (last visited Mar. 29, 2014).} Apple has recently mandated that any update made to an app must also include an update to make the app compatible with Apple’s new device versions.\footnote{\textit{Make Your Apps Look Great on the Retina Display and iPhone 5}, \textsc{Apple} (Mar. 21, 2013), \url{https://developer.apple.com/news/?id=3212013b} (“Starting May 1, new apps and app updates submitted to the App Store must be built for iOS devices with Retina display and iPhone apps must also support the 4-inch display on iPhone 5.”).} If a manufacturer faces FDA restrictions from updating their app for new operating systems or platform versions, the manufacturer may find themselves facing conflicting regulations where they cannot comply with all FDA regulations as they risk violating FDA quality system regulations by not fixing the bugs they have found or if they fix the bugs they will violate their obligations to only have their product run on an earlier operating system or platform.

While the FDA’s Guidance on mobile medical applications focuses on the types of applications the FDA will regulate and provides some direction on regulatory requirements, further guidance on some of the practical problems that regulated devices will face is required. First, the FDA should clarify that all changes require manufacturer verification and validation, pursuant to the quality system regulations, prior to being released.

Second, the FDA should clarify whether the clearance and approval of mobile medical apps is specific to the operating system version the app runs on. As detailed above, if apps are only approved for specific operating systems multiple issues will arise, including what the manufacturers obligations are to ensure that the app is not used on newer unapproved operating systems. In the event that mobile medical apps may be used with newer operating systems, the FDA should clarify the manufacturer’s obligations should the new operating system be released prior to the manufacturer completing its design control obligations.\footnote{It is the author’s opinion that such an approach would result in fewer complications.}

Third, the FDA should clarify whether the clearance and approval of mobile medical apps is specific to the type of platform the app
operates on.\textsuperscript{255} It is the author’s position that the FDA should create two categories of mobile medical apps: (1) where the medical mobile app relies on specific aspects of the platforms hardware that is specific to one platform (ex: camera, adaptor port, size/shape), and (2) where the app does not rely on hardware specific to the platform. In the first instance, where the app relies on unique hardware, the approval or clearance should be specific to the platform type and new clearance or a supplemental PMA should be filed for approval of the use of the app with the changed design of the platform. However, where the app does not rely on hardware specific to the platform, changes to the platform type should be addressed similar to changes in the operating system version. Clarification will be required to inform manufacturers of whether they have any obligations to ensure that the app is not being used on new platforms prior to FDA approval/clearance of these uses.

D. Updating Software on Combination Products

FDA requirements for the updating of software will be complicated where the software to be updated is a part of a combination product, especially where the combination product was originally approved as a drug by CDER or as a biological product by the CBER. Where the combination product is approved by the CDRH, the types of procedure are likely to be similar to the procedure for gaining approval or clearance for changes to a stand-alone medical device. However, where the combination product was originally approved as a drug or biological product, two potential issues that may arise: (1) the type/format of submission for a software change to a combination product may differ from where the same software change is made to a stand-alone device, and (2) the need for FDA permission to make a software change may differ from where the same software change is made to a stand-alone device.

FDA Guidance thus provides some assistance in determining what type of submission to make in response to postmarket changes.\textsuperscript{256} However, because the Guidance treats all combination products as if their device components would be approved under a PMA this approach fails to take into consideration the reality that most devices proceed to market via 510(k) clearance and not PMA. Additionally,

\textsuperscript{255} FDA Guidance recognizes that app risks may be specific to the platform but does not address platform based specificity of approval or clearance, see U.S. FOOD & DRUG ADMIN., \textit{supra} note 31, at 6-7.

\textsuperscript{256} U.S. FOOD & DRUG ADMIN., \textit{supra} note 162, at 4, 6.
treating all device components as PMA approved devices may result in software changes being subject to additional requirements when the component the change is made to is part of a combination device versus being a stand-alone device. For example consider how the regulatory requirements would differ if the same software updates were made to a stand-alone insulin pump versus the same insulin pump containing a novel insulin-like drug and approved as a combination product via a NDA. Imagine that the stand-alone insulin pump was declared substantially equivalent to a predicate device and cleared through the 510(k) pathway. The proposed software update does not affect the safety and effectiveness of the device and therefore, because the stand-alone pump was cleared through the 510(k) pathway, does not require an additional clearance submission. The manufacturer would have no obligation to seek approval or notify the FDA. The combination product in this example, however, was not cleared through a 510(k) pathway, but through a NDA to CDER. To follow the Guidance on what submission must be made to CDER for a change to a device component of a combination product, one is required to consider what type of submission would be required under the device regulation if the device were approved under a PMA application. In the case of a PMA approved device, the same software modification would require a PMA period report, even if the safety and effectiveness of the device were not affected. The manufacturer of the combination product would thus be required to submit an annual report to the FDA under the drug regulation detailing the minor change, but would have no similar obligation to report the same change made to a stand-alone pump. The varying regulatory requirements for the same software change, dependent on whether the marketed item is a combination or stand-alone product, has the potential to further complicate the issue of when software updates can be made and what requirements must be fulfilled to do so.

As combination products become more complex and increasingly contain software components, manufactures will have to be vigilant to ensure that they are complying with all of their obligations under the FDAs regulations. The FDA’s 2013 Draft Guidance takes initial steps to assisting manufacturers in determining their obligations. However, further guidance, particularly in dealing with 510(k) cleared devices, will be useful.

257 Although insulin and insulin pumps are currently approved as two separate items and not considered to be combination products, there is a potential that such items could be marketed together as a combination product.

258 U.S. FOOD & DRUG ADMIN., supra note 162, at 4, 6.
IV. Conclusion

Software updates are instrumental to the continual smooth functioning of many medical devices, and manufactures should be encouraged to fix problems associated with their devices through the issuance of such updates. Although there are points that the FDA could clarify on the regulation of proprietary device software and combination product software, no major concerns have arisen in these areas and a wait-and-see approach may be most useful.

With respect to the updating of security patches or anti-virus software, the FDA should clarify that such updates will not require its permission, although the manufacturer will have an obligation to verify and validate the update. Because the verification/validation requirement may provide a financial barrier to manufacturers issuing such security updates, the FDA should take a position on what extent a manufacturer is responsible for malware issues faced by users of the manufacture’s device. Although the FDA has generally taken a non-prescriptive approach to quality system regulation, given the numerous reports of malware causing harm, this situation requires that the FDA provide specific instruction as to whether manufacturers have an obligation to protect their devices from malware by issuing security updates, or whether users are required to protect the devices from malware by keeping them behind firewalls. Both options will likely have severe financial implications, either on the manufacture in the first instance or the users in the latter. However, these implications are likely outweighed by the liability that may result from a massive cybersecurity attack.

The area of mobile medical apps is likely to be a huge growth area in the medical device field. Furthermore, this is an area where manufactures have less flexibility over the control of their devices due to requirements set out by app distributors. Substantial clarification will be required in this area to address potential conflicts between FDA regulations and distributor requirements. Most importantly the FDA needs to clarify whether apps approved by the FDA are platform model specific and/or operating system specific, and if a manufacture has any obligation to prevent a user form using the app on an unapproved platform model or operating system.

Software has the potential to revolutionize many medical devices. Furthermore, many medical devices that contain software require updates to add features, and fix bugs or security issues as they arise. Clear and understandable procedures through which manufactures may bring their changed devices to market will therefore benefit the medical device industry.
KNOWING IS HALF THE BATTLE: HOW LATE IS TOO LATE TO MEET THE KNOWLEDGE ELEMENT WHEN PLEADING INDIRECT PATENT INFRINGEMENT?

Jack Burns†

I. INTRODUCTION ............................................................. 420
II. BACKGROUND .................................................................... 421
   A. HISTORY ........................................................................ 421
   B. CASE ANALYSIS ............................................................. 424
      1. Cases Finding Pre-Complaint Knowledge Not Required to Recover for Indirect Infringement........ 425
      2. Cases Requiring Pre-Complaint Knowledge to Recover for Indirect Infringement ..................... 430
III. WHY FEDERAL CIRCUIT REVIEW IS NECESSARY ... 436
IV. CONCLUSION ..................................................................... 438

ABSTRACT

The recent United States Supreme Court case Global-Tech Appliances, Inc. v. SEB S.A.1 did much to clarify the pleading requirements of an adequate indirect infringement claim. In that case, for the first time, the Supreme Court made clear that both forms of indirect infringement—induced infringement as well as contributory infringement—require that the defendant have knowledge of the underlying patent.

However, for as much as the Supreme Court’s Global-Tech decision illuminates the indirect infringement knowledge requirement, it leaves open the important question of when the defendant must have knowledge of the patent. This remains a highly contentious and heavily divided issue among the district courts. Many district courts

† Jack Burns is a litigation attorney for Greenberg Traurig, LLP and a former law clerk for the Honorable Judge Procter Hug, Jr. on the U.S. Court of Appeals for the Ninth Circuit.

find that only pre-suit knowledge of the underlying patent is sufficient to maintain an indirect infringement suit. On the other hand, several other district courts find that post-suit knowledge alone is sufficient, but damages are available only for conduct that occurs after the defendant has the requisite knowledge of the patent. Both camps have heavy criticism for the other, and both camps have labeled their own position to be the “majority” position. This deep split screams for Federal Circuit review. In the interim, the district courts are left to their own devices to choose the side on which they fall.

This Article analyzes the merit of both schools of thought. It starts by providing a brief history of the knowledge element of an indirect patent infringement suit. It also provides a summary of several cases on each side of the fence and the reasoning the courts have employed in reaching their decisions.
I. INTRODUCTION

Under the doctrine of indirect infringement, a defendant is liable for merely inducing another to infringe on a patent or, alternatively, for contributing to the infringement of a patent. This expansive ground for liability stands in stark contrast to the doctrine of direct infringement, which requires every single claim limitation to read on an allegedly infringing product. In other words, to prevail on a claim for direct infringement, “a patentee must supply sufficient evidence to prove that the accused product or process contains . . . every limitation of the properly construed claim.”

However, unlike direct infringement, indirect infringement is not a strict liability tort. Thus, while a defendant can be liable for direct infringement without even knowing of the patent’s existence, liability for indirect infringement requires more. It requires knowledge that the infringing acts constitute patent infringement. Knowledge of patent infringement, in turn, requires knowledge that the underlying patent exists. But when must a defendant have this knowledge in order to be liable for indirect infringement? Can a claim for indirect infringement stand when the first time the defendant learns of the patent is in the same complaint alleging the defendant is liable for indirect infringement? District courts across the country are divided on this very question, and the issue is more than ripe for Federal Circuit review. While district courts appear to be evenly divided on the issue,

---

3 35 U.S.C. § 271(c) (2012) (stating: “Whoever offers to sell or sells within the United States or imports into the United States a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer.”).
4 35 U.S.C. § 271(a) (2012) (stating “whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States . . . infringes the patent”).
5 Seal–Flex, Inc. v. Athletic Track & Court Constr., 172 F.3d 836, 842 (Fed. Cir. 1999).
7 Global–Tech, 131 S. Ct. at 2068; Akamai, 692 F.3d at 1308.
both approaches have been labeled as the majority approach.\textsuperscript{8}

This Article explores the heavily divided question of whether a case for direct infringement requires defendant’s pre-complaint knowledge of the patent. Part Two of this Article provides the background behind the indirect infringement knowledge requirement, including a brief history of the split and an analysis of the cases that have ruled on the issue. Part Three discusses the merit of each approach and emphasizes why Federal Circuit review is necessary to resolve this issue once and for all.

II. BACKGROUND

A. History

35 U.S.C. § 271(c) “was designed to codify in statutory form principles of contributory infringement which had been part of our law for about 80 years.”\textsuperscript{9} “Before 1952, both the conduct now covered by § 271(b) (induced infringement) and the conduct now addressed by § 271(c) (sale of a component of a patented invention) were viewed as falling within the overarching concept of ‘contributory infringement.’”\textsuperscript{10} Indeed, induced infringement “was treated as evidence of contributory infringement, that is, the aiding and abetting of direct infringement by another party.”\textsuperscript{11}

“While both the language of § 271(b) and the pre-1952 case law that this provision was meant to codify are susceptible to conflicting interpretations”\textsuperscript{12} regarding whether knowledge of the patent was required to be liable for contributory infringement, the Supreme Court’s decision in \textit{Aro Manufacturing Co. v. Convertible Top Replacement Co.} (“\textit{Aro II}”) settled that question.\textsuperscript{13}

In \textit{Aro II}, plaintiff Convertible Top Replacement owned a patent covering a top-structure for convertible automobiles.\textsuperscript{14} Ford had no license or authority under Convertible Top Replacement’s patent

\textsuperscript{8} See Brandywine Commc’ns Techs., LLC v. T-Mobile USA, Inc., 904 F. Supp. 2d 1260, 1267 (M.D. Fla. 2012) (declaring that the “weight of authority” required pre-suit knowledge). \textit{But see} Rembrandt Soc. Media, LP v. Facebook, Inc., 950 F.Supp.2d 876, 881 (E.D. Va. 2013) (“[A] majority of district courts considering this issue have held that post-suit knowledge (i.e., knowledge provided by the filing of the lawsuit) satisfies the knowledge element for indirect infringement.”).

\textsuperscript{9} Global–Tech, 131 S. Ct. at 2065-66 (quotations omitted).

\textsuperscript{10} \textit{Id.} at 2066.

\textsuperscript{11} \textit{Id.} at 2067.

\textsuperscript{12} \textit{Id.}

\textsuperscript{13} \textit{Aro Mfg. Co. v. Convertible Top Replacement Co.} (\textit{Aro II}), 377 U.S. 476, 482 (1964).

\textsuperscript{14} \textit{Id.} at 478.
during the relevant time period. Aro Manufacturing Company produced fabric components to replace worn-out convertible tops, and Aro’s products were specially tailored for installation on particular vehicles, including those covered by Convertible Top Replacement’s patent. Aro did not have a license under Convertible Top Replacement’s patent. Convertible Top Replacement brought an action, which sought, among other things, to enjoin Aro’s alleged infringement and contributory infringement. The Supreme Court granted certiorari to address the question of “whether Aro is liable for contributory infringement, under 35 U.S.C. § 271(c), with respect to its manufacture and sale of replacement fabrics for the Ford cars.”

The Supreme Court, in a splintered majority opinion, began its inquiry by determining whether the Ford car owners, by replacing the fabric on the top, committed direct infringement of Convertible Top Replacement’s patent. The Court noted that Ford had infringed the patent by making and selling cars infringing on the patent. The Court noted further that, because Ford lacked authority to use or sell the patented top, by selling the vehicles to its purchasers, Ford conferred no license to use the patent, and therefore the purchasers’ use of the patented top structure was direct infringement under 35 U.S.C. § 271(a). Having established that the Ford owner’s use of the top infringed on Convertible Top Replacement’s patent, the Court elaborated that “[i]f the owner’s use infringed, so also did his repair of the top-structure, as by replacing the worn-out fabric component. Where use infringes, repair does also, for it perpetuates the infringing use.”

Next, the Court turned to the question of “whether Aro, as supplier

---

15 Id. at 478-79.
16 Id. at 479.
17 Id.
18 Id. In an earlier case, Aro Mfg. Co. v. Convertible Top Replacement Co. (Aro I), 365 U.S. 336 (1961), the Supreme Court dealt with the question of whether replacement of the fabric portions of the convertible tops constituted infringing ‘reconstruction’ or permissible ‘repair’ of the patented combination when the automobile manufacturer—General Motors—had a license with the patentee. Aro I, 365 U.S. at 339-41. The Court held for Aro, concluding that their act was mere repair and not reconstruction. Id. However, Aro I did not prevent liability for Aro in Aro II because “when the structure is unlicensed, as was true of the Ford cars, the traditional rule is that even repair constitutes infringement.” Aro II, 377 U.S. at 479-80.
19 Aro II, 377 U.S. at 481.
20 Id. at 483.
21 Id. at 484.
22 Id.
23 Id.
of replacement fabrics for use in the infringing repair by the Ford car owners, was a contributory infringer under § 271(c) of the Patent Code. 24 The Court found that Aro was a contributory infringer. 25 In doing so, the Court noted “the language of § 271(c) presents a question, apparently not noticed by the parties or the courts below, concerning the element of knowledge that must be brought home to Aro before liability can be imposed.” 26

The Court specifically reviewed whether knowledge of the infringed patent and the infringing activity must be known by the contributory infringer. 27 “On this question a majority of the Court [was] of the view that § 271(c) does require a showing that the alleged contributory infringer knew that the combination for which his component was especially designed was both patented and infringing.” 28 The majority stated that a letter dated January 2, 1954 informed Aro of the relevant patent and that General Motors had a license, but no one else did. 29 Thus, the majority of the Court held Aro had “no defense with respect to replacement-fabric sales made after January 2, 1954,” but “[w]ith respect to any sales that were made before that date, . . . Aro [could not] be held liable in the absence of a showing that at that time it had already acquired the requisite knowledge that the Ford car tops were patented and infringing.” 30

The majority’s view regarding the requisite knowledge divided the Supreme Court and was joined by five of the nine Justices. 31 The remaining four Justices “[were] of the view that the knowledge Congress meant to require was simply knowledge that the component was especially designed for use in a combination and was not a staple article suitable for substantial other use, and not knowledge that the combination was either patented or infringing.” 32

In Global-Tech, the Supreme Court noted that although Aro II involved a heavily divided Court on the question of whether

24 Id. at 485.
25 Id. at 485-88.
26 Id. at 488.
27 Id. (asking: “Was Aro ‘knowing’ within the statutory meaning because—as it admits, and as the lower courts found—it knew that its replacement fabrics were especially designed for use in the 1952-1954 Ford convertible tops and were not suitable for other use? Or does the statute require a further showing that Aro knew that the tops were patented, and knew also that Ford was not licensed under the patent so that any fabric replacement by a Ford car owner constituted infringement?”).
28 Id.
29 Id. at 489-90.
30 Id. at 490-91.
31 Id. at 488 n.8.
32 Id.
knowledge of both the patent and its infringement was required and “there is much to be said in favor of both views expressed in Aro II, the ‘holding in Aro II has become a fixture in the law of contributory infringement.’”\textsuperscript{33} Based on this and “the special force of the doctrine of \textit{stare decisis} with regard to questions of statutory interpretation,”\textsuperscript{34} the Court, in an opinion by Justice Alito, did not disturb “the premise that § 271(c) requires knowledge of the existence of the patent that is infringed.”\textsuperscript{35}

The \textit{Global-Tech} Court extracted from the \textit{Aro II} premise that “the same knowledge is needed for induced infringement under § 271(b).”\textsuperscript{36} The Court put great weight on the fact that both induced infringement and contributory infringement “have a common origin in the pre-1952 understanding of contributory infringement, and the language of the two provisions creates the same difficult interpretive choice.”\textsuperscript{37} The Court continued, “[i]t would thus be strange to hold that knowledge of the relevant patent is needed under § 271(c) but not under § 271(b).”\textsuperscript{38} For that reason, the Court held “that induced infringement under § 271(b) requires knowledge that the induced acts constitute patent infringement.”\textsuperscript{39} Therefore, it is established that in order to survive a motion to dismiss on a claim for indirect infringement, a complaint must contain facts plausibly showing that the defendant “specifically intended their customers to infringe the [relevant] patent and knew that the customer’s acts constituted infringement.”\textsuperscript{40}

\textbf{B. Case Analysis}

While it is established that knowledge of the relevant patent is necessary in order to maintain a claim for indirect infringement of that patent, district courts across the country are split on whether post-suit knowledge of the patent, gained through receiving the complaint in the case, is sufficient to satisfy the knowledge requirement. While many courts answer that question in the negative, many others find that pre-suit knowledge is not required. Indeed, there is even a split as to

\small
\begin{itemize}
\item \textsuperscript{33} Global–Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2068 (2011).
\item \textsuperscript{34} \textit{Id.} (quotations omitted).
\item \textsuperscript{35} \textit{Id.}
\item \textsuperscript{36} \textit{Id.}
\item \textsuperscript{37} \textit{Id.}
\item \textsuperscript{38} \textit{Id.}
\item \textsuperscript{39} \textit{Id.}
\item \textsuperscript{40} \textit{In re} Bill of Lading Transmission & Processing Sys. Patent Litig., 681 F.3d 1323, 1339 (Fed. Cir. 2012).
\end{itemize}
which view is the majority view. The following is a summary of the major cases for each stance.

1. **Cases Finding Pre-Complaint Knowledge Not Required to Recover for Indirect Infringement**

   a. **Groupon Inc. v. MobGob LLC**

   *Groupon Inc. v. MobGob LLC* is the first of three cases from the U.S. District Court for the Northern District of Illinois holding that defendant’s pre-complaint knowledge of the patent is not required to maintain a suit for indirect infringement. Both plaintiff Groupon and defendant MobGob used their websites to promote the goods and services of others, and both Groupon’s and MobGob’s websites featured coupons and discounts. Groupon sued MobGob, alleging that MobGob indirectly infringed Groupon’s patent for an “On-Line Marketing System and Method.” MobGob filed a motion to dismiss, focusing on the knowledge and intent elements. MobGob argued that Groupon’s allegations were insufficient to establish the knowledge element because Groupon simply alleged that MobGob had knowledge of the patent “upon information and belief.” The court disagreed with MobGob.

   District Judge Hibbler explained that “[i]t is reasonable to infer that MobGob had actual knowledge of Groupon’s public patent (or at the very least that it has such knowledge now and allegedly continues its activities).” In other words, according to Judge Hibbler, general allegations of knowledge are sufficient to survive a motion to dismiss because, at the very least, the defendant had knowledge of the patent by learning of it in the complaint. While *Groupon* pre-dated the Supreme Court’s decision in *Global-Tech*, as seen below, courts continue to rely heavily on the *Groupon* decision.

---

43 Id. at *1.
44 Id.
45 Id. at *3.
46 Id.
47 Id.
48 Id.

In *Trading Technologies International, Inc. v. BCG Partners, Inc.*,\(^{49}\) plaintiff Trading Technologies International sued numerous entities in the business of providing electronic trading software for indirectly infringing Trading Technologies’ electronic trading patents.\(^{50}\) Citing *Groupon*, the court denied the defendants’ motion to dismiss Trading Technologies’ indirect infringement claims based on lack of pre-suit knowledge.\(^{51}\) District Judge Kendall explained that she “believe[d] the *Groupon* approach [to be] the more practical one, assuming the plaintiff can plead that the defendant continues to sell its infringing product.”\(^{52}\) The court explained further that it “[saw] no reason why a defendant who is directly infringing on a product should avoid liability for an indirect infringement claim when it continues to sell the allegedly infringing product and encourages others to infringe, simply because it happened to learn of the patent in connection with a lawsuit.”\(^{53}\)


In *Intellect Wireless Inc. v. Sharp Corp.*,\(^{54}\) plaintiff Intellect Wireless brought a patent infringement suit based on apparatus and method patents that included features for displaying the photograph and phone number of the sender of cellular telephone messages.\(^{55}\) The defendants—manufacturers of wireless communications devices—sought summary judgment on plaintiff’s indirect infringement claim, because the plaintiff relied only on post-complaint activity.\(^{56}\) In fact, the *only* evidence plaintiff presented as to indirect infringement was advertisements and user manuals that the defendants published and disseminated after the date of the complaint.\(^{57}\) The court noted that “[t]he parties appear[ed] to agree that Defendants first became aware


\(^{50}\) Id. at *1, *4.

\(^{51}\) Id. at *4-5.

\(^{52}\) Id. at *4.

\(^{53}\) Id.


\(^{55}\) Id. at *1.

\(^{56}\) Id.

\(^{57}\) Id. at *2.
of the patents-in-suit when [plaintiff] filed its complaint.”

Relying heavily on Trading Technologies International, Inc. v. BCG Partners, Inc., District Judge Pallmeyer’s order held that a defendant is liable for an indirect infringement claim when it “continue[s] to promote infringing uses of their products after learning about the patents,” even when the defendant learned of the patent from the complaint in the lawsuit. Therefore, the court held that “[d]efendants’ knowledge of the patent as of the time of the suit’s commencement can satisfy the knowledge requirement for conduct that post-dates the date of the complaint.”

d. Walker Digital, LLC v. Facebook, Inc.

The U.S. District Court for the District of Delaware is much more divided on the topic. The first time the court found that pre-suit knowledge was not required was in Walker Digital, LLC v. Facebook, Inc. There, plaintiff Walker Digital sued numerous website operators including Fandango, Amazon, eBay, and Zappos.com under its patent entitled “Method and Apparatus for Facilitating Electronic Commerce Through Providing Cross-Benefits During a Transaction.” Walker Digital claimed that Amazon and Zappos indirectly infringed on their patent by “making, using, offering for sale, selling and/or importing apparatuses and/or practicing methods that provide cross-benefits during a transaction including, but not limited to, that provide [defendants’] users/customers the ability to receive a benefit in connection with a purchase via a cross-promotion.”

Amazon and Zappos moved to dismiss Walker Digital’s claims, and District Judge Robinson denied the motion to dismiss, concluding that Walker Digital’s allegations satisfied the requirements of Global-Tech. The court reasoned “there is no legal impediment to having an indirect infringement cause of action limited to post-litigation conduct” and found it instructive that “the fundamental purpose of

---

58 Id. at *11.
61 Id.
63 Id. at 565.
64 Id. at 561.
65 Id. at 565.
asserting indirect infringement [is] . . . to ensure that the patentee can recover full compensation for any damages suffered as a result of infringement." 66 Therefore, Judge Robinson found that “the only substantive consequence of allowing [indirect infringement claims based on post-suit knowledge] to go forward” was “[t]he fact that Walker Digital would be prohibited from collecting damages related to indirect infringement for any pre-knowledge (e.g., pre-filing) conduct.” 67 The court also noted that “it is important to keep in mind that the Supreme Court was reviewing Global-Tech post-trial and did not speak to the pleading requirements for indirect infringement under Rule 8 [of the Federal Rules of Civil Procedure].” 68

e. SoftView, LLC v. Apple Inc.

In SoftView, LLC v. Apple Inc., 69 plaintiff SoftView sued multiple mobile device manufacturers for infringement of patents entitled “Scalable Display of Internet Content on Mobile Devices.” 70 The defendants filed a motion to dismiss, contending that SoftView’s indirect infringement claims should be dismissed for failure to state a claim because SoftView had not plausibly alleged defendants’ pre-suit knowledge of the patents-in-suit. 71 District Judge Stark held that SoftView adequately alleged pre-suit knowledge of the patents-in-suit by most defendants, but found that SoftView had failed to plausibly allege such knowledge by defendant Kyocera. 72

In determining whether an indirect infringement claim required pre-suit knowledge of the patent, Judge Stark noted that there was divided precedent, even within the U.S. District Court for the District of Delaware. 73 Ultimately, the court sided with the plaintiff, concluding “[o]n balance, the Court agrees with SoftView’s position that the filing of a complaint is sufficient to provide knowledge of the patents-in-suit for purposes of stating a claim for indirect infringement occurring after the filing date.” 74 The court explained that “[i]n the

66 Id.
67 Id.
68 Id.
70 Id. at *1.
71 Id. at *5.
72 Id. at *6-7.
73 Id. at *7.
74 Id. (quoting Apple Computer, Inc. v. Unova, Inc., No. Civ.A. 03-101-JJF, 2003 WL 22928034, at *5 (D. Del. Nov. 25, 2003) (“In its Amended Complaint, Apple has alleged that, since the initial pleading, Intermec and Unova were aware of
continued . . . 
Court’s view, an accused infringer is on notice of the patent(s)-in-suit once an initial pleading identifies the patents-in-suit, and a patentee that successfully proves the remaining legal elements of indirect infringement [sic] is entitled to recover for any post-filing indirect infringement of those patents.”\(^75\)

\(^f\) Apeldyn Corp. v. Sony Corp.

District Judge Robinson cemented her previous *Walker Digital* decision in *Apeldyn Corp. v. Sony Corp.*\(^76\) There, plaintiff Apeldyn sued Sony for infringement of a patent directed to the response time of liquid crystal material in Liquid Crystal Display modules (“LCDs”). \(^77\) In opposing Sony’s motion to dismiss Apeldyn’s indirect infringement claim, Apeldyn asserted that “Sony knew of the ‘382 patent at least as of the filing of the complaint [in a previous case between Sony and Apeldyn] and, armed with that knowledge, has continued to indirectly infringe by making and/or selling infringing LCD products in the United States.” \(^78\)

After a copy-and-paste recitation of the court’s reasoning in *Walker Digital*, the court denied Sony’s motion to dismiss. \(^79\) The court summarized its ruling as follows: “if a complaint sufficiently identifies, for purposes of Rule 8, the patent at issue and the allegedly infringing conduct, a defendant’s receipt of the complaint and decision to continue its conduct despite the knowledge gleaned from the complaint satisfies the requirements of *Global-Tech*.” \(^80\)

\(^g\) InMotion Imagery Technologies v. Brain Damage Films

In *InMotion Imagery Technologies v. Brain Damage Films*,\(^81\) plaintiff InMotion accused thirteen defendants of infringing a patent for a “Picture–Based Video Indexing System.” \(^82\) Defendant Galaxy

\(^77\) *Id.* at 570.
\(^78\) *Id.* at 573.
\(^79\) *Id.* at 573-74.
\(^80\) *Id.* at 574.
\(^82\) *Id.* at *1.
filed a motion to dismiss the induced infringement claims based on their lack of knowledge of the patents. District Judge Gilstrap denied the motion and explained “[f]ailing to allege pre-suit knowledge of the patent is not a basis to dismiss Plaintiff’s indirect infringement claims; as it cannot be disputed that Plaintiff does sufficiently plead that the Moving Defendants had knowledge of the asserted patent for at least some time during the infringing period.”

**h. Symantec Corp. v. Veeam Software Corp.**

*Symantec Corp. v. Veeam Software Corp.* involved plaintiff Symantec and defendant Veeam—competitor providers of backup and recovery software. Symantec alleged that Veeam had infringed its patents for “distinct, remote backup” of a machine on a separate storage device and “for backup and restoration of an entire machine on a network in the event that the client should become incapable of booting up on its own.” District Judge Illston, quoting the *Intellect Wireless* and *Trading Technologies* line of cases from the Northern District of Illinois, rejected Veeam’s motion to dismiss for insufficient allegations of knowledge. “The Court [found] that plaintiff ha[d] adequately pled knowledge of alleged infringement as of the date of the complaint . . . [and] construe[d] the complaints as covering contributory infringement for post-filing conduct, where the defendant’s knowledge ha[d] been adequately alleged.”

**2. Cases Requiring Pre-Complaint Knowledge to Recover for Indirect Infringement**

**a. Proxyconn Inc. v. Microsoft Corp.**

In *Proxyconn Inc. v. Microsoft Corp.*, District Judge David O. Carter of the U.S. District Court for the Central District of California granted defendants’ motion to dismiss plaintiff Proxyconn’s claim that

---

83 Id. at *3.
86 Id. at *1.
87 Id.
88 Id. at *4.
89 Id.
the defendants indirectly infringed on their method patent through
defendants’ making and selling computer systems. 91 Proxyconn
alleged that each defendant had knowledge of the underlying patent
“[s]ince at least the filing of the complaint” and conceded that it could
“only specifically allege that [d]efendants had knowledge of the
patent-in-suit as of the filing of the original complaint.” 92 In granting
the defendants’ motion to dismiss Proxyconn’s indirect infringement
claim, the court explained:

Plaintiff’s argument requires this Court to bootstrap the
knowledge Defendants now have based on Plaintiff’s
filing of the Complaint onto defendant’s acts before
Plaintiff filed its complaint. Yet, a defendant can not
be held liable because it induced or contributed to
another’s acts before the defendant had knowledge,
because to do so effectively holds a defendant liable for
acts it did without knowledge. 93

The court further reasoned that “requiring a [p]laintiff to plead
knowledge based on facts other than the filing of the present lawsuit
furthers judicial economy and preserves parties’ resources by
encouraging resolution prior to filing a lawsuit” and also explained
that “[p]re-litigation attempts at resolution are especially desirable in
patent cases, which are often expensive and thus resolved by
settlement.” 94 The court stated further that “Plaintiff could have
notified Defendants of their alleged infringement and sought an
amicable resolution at any time prior to filing this suit” and the
defendants “should not be punished for Plaintiff’s failure to do so.” 95
The Proxyconn court next distinguished Trading Technologies and
Groupon. 96

The court found Trading Technologies factually distinguishable
because “the complaint [in Trading Technologies] alleged additional facts other than the filing of the complaint that established the
defendants’ knowledge.” 97 The court found Groupon factually
distinguishable because “the [Groupon] complaint alleged that the
defendant had knowledge but did not specify when it was acquired;
the courts reasoned that allegations without a time period were

91 Id. at *1, *2-7.
92 Id. at *2, *5.
93 Id. at *5.
94 Id.
95 Id.
96 Id. at *6.
97 Id.
sufficient because a motion to dismiss requires all inferences to be drawn in the plaintiff’s favor.”

The court also criticized the cases that hold pre-complaint knowledge of the patent by the defendant is not required to maintain a suit for indirect infringement as being “based on an incorrect understanding of the consequences of granting a motion to dismiss.”

The court explained that “[i]n Trading Technologies, the court denied the motion to dismiss because it feared that granting the motion would allow a defendant to avoid liability for an indirect infringement claim simply because it happened to learn of the patent in connection with a lawsuit.” However, the Proxyconn court found this concern “completely unfounded.” Judge Carter went on to explain that “nothing prevents a plaintiff from filing a new lawsuit alleging that the knowledge requirement is established because the defendant is aware of the previous lawsuit, . . . [and] Federal Rule of Civil Procedure 15(d) provides a procedure for pleading post-suit facts.”

The Proxyconn court also criticized the reasoning from Walker Digital that the interests of judicial economy favor denying a motion to dismiss because by the time the motion to dismiss has been filed, the defendant in fact has the requisite knowledge. Judge Carter explained that “[s]uch a view gives too little weight to the judicial inefficiencies and parties’ expenses in litigating potentially meritless claims.” Judge Carter argued that, under the alternative system, even if a defendant ceased all infringing activity on the day the complaint is filed, the unfortunate defendant would have to expend vast resources to come to the summary judgment stage of litigation before the expensive and meritless indirect infringement claim could be dismissed. Thus, in dismissing Proxyconn’s indirect infringement claim, the court adopted the rule that “a complaint fails to state a claim for indirect patent infringement where the only allegation that purports to establish the knowledge element is the allegation that the complaint itself or previous complaints in the same lawsuit establish the defendant’s knowledge of the patent.”

---

98 Id.
99 Id.
100 Id. (internal quotation marks omitted).
101 Id.
102 Id.
103 Id. at *7 (quoting Walker Digital, LLC v. Facebook, Inc., 852 F. Supp. 2d 559, 566 n. 11 (D. Del. 2012)).
105 Id.
106 Id.
b. Brandywine Communications Technologies, LLC v. T-Mobile USA, Inc.

Brandywine Communications Technologies, LLC v. T-Mobile USA, Inc.\(^{107}\) involved a patent for a “Simultaneous Voice/Data Answering Machine.”\(^{108}\) There, plaintiff Brandywine alleged that T-Mobile indirectly infringed on the patent by making, using, selling, and offering for sale certain mobile phone models such as the “Comet, G2x, Sidekick 4G, and the HTC Wildfire S.”\(^{109}\) Plaintiff alleged that T-Mobile had knowledge of the patent since at least the day it was served with the original complaint in the case.\(^{110}\) The court, in an order by Judge Honeywell, granted T-Mobile’s motion to dismiss.\(^{111}\) The court reasoned that “because notice of the patent is necessarily provided by a complaint, finding that a complaint provides sufficient knowledge for induced infringement would vitiate the Supreme Court’s holding in Global–Tech that an allegation of knowledge of the patent is required to state a claim for induced infringement.”\(^{112}\) The order characterized this as the majority approach, stating that “[t]he weight of authority addressing the knowledge required for indirect infringement, especially following the Supreme Court’s decision in Global–Tech, requires a plaintiff to allege that defendant had pre-suit knowledge of the patents-in-suit.”\(^{113}\)

c. Xpoint Technologies, Inc. v. Microsoft Corp.

Xpoint Technologies, Inc. v. Microsoft Corp.\(^{114}\) dealt with a patent for “a direct data-distribution system and method for program-controlled, direct transfer of data along a bus or data pathway between peer input/output (‘I/O’) devices in a data-processing apparatus or data-processing network.”\(^{115}\) Such a direct data transfer allegedly “optimizes the speed and efficiency of an apparatus or network by allowing data to bypass the central processing unit (‘CPU’) and thereby preserve the CPU’s capacity for other applications.”\(^{116}\) This

\(^{108}\) Id. at 1262.
\(^{109}\) Id. at 1262-63.
\(^{110}\) Id. at 1263.
\(^{111}\) Id. at 1262.
\(^{112}\) Id. at 1268-69.
\(^{113}\) Id. at 1267 (citations omitted).
\(^{114}\) Xpoint Techs., Inc. v. Microsoft Corp., 730 F. Supp. 2d 349 (D. Del. 2010).
\(^{115}\) Id. at 351 (internal marks omitted).
\(^{116}\) Id.
technology could be used on “electronic devices like cell phones, personal media players, personal computers, and global positioning system (‘GPS’) devices.” 117 Xpoint sued multiple technology companies alleging indirect infringement and “argue[d] that defendants had knowledge of the [relevant] patent at least since the date of the suit.” 118 The court, in an order by Judge Robinson, found this insufficient and granted defendants’ motion to dismiss, explaining that “knowledge after filing of the present action is not sufficient for pleading the requisite knowledge for indirect infringement.” 119 Notably, Judge Robinson also presided over Apeldyn, where she switched sides and held that post-suit knowledge was sufficient. 120

d. Aguirre v. Powerchute Sports, LLC

In Aguirre v. Powerchute Sports, LLC, 121 plaintiff Aguirre alleged the indirect infringement of his patent concerning a physical conditioning aid for golfers and sued defendant sellers of allegedly infringing products. 122 Citing Xpoint, the court held that knowledge of the patent was insufficiently pled and “[t]o the extent Aguirre relies on knowledge of [his] patent after the lawsuit was filed, such knowledge is insufficient to plead the requisite knowledge for indirect infringement.” 123

e. Select Retrieval, LLC v. Bulbs.com Inc.

Select Retrieval, LLC v. Bulbs.com Inc. 124 went even further than Proxyconn and the other cases requiring pre-suit knowledge of the patent. There, defendant Bulbs.com argued that plaintiff Select Retrievals’ complaint did not adequately state a claim for indirect infringement because the complaint relied “on the filing of a prior lawsuit to satisfy the knowledge element.” 125 The district court explained that “[i]n general, relying on the filing of a suit to show that a defendant had knowledge of the existing patent is not sufficient for

117 Id.
118 Id. at 357 (internal marks omitted).
119 Id.
122 Id. at *1.
123 Id. at *3.
125 Id. at *5.
pleading an inducement claim.” However, the court went so far as to find that even knowledge stemming from a prior lawsuit would be insufficient.

f. Secured Mail Solutions, LLC v. Advanced Image Direct, LLC

Judge Carter of the U.S. District Court for the Central District of California confirmed his Proxyconn decision in early 2013 in the case of Secured Mail Solutions, LLC v. Advanced Image Direct, LLC.128 There, perhaps secure in the knowledge that they were before the very same judge that had adamantly criticized courts that had permitted post-complaint knowledge to suffice, the defendants argued:

Plaintiff’s argument that ‘discovery may uncover facts that could establish knowledge’ before this lawsuit is rank speculation. This Court should not condone Plaintiff’s strategy to file first and then troll on a fishing expedition to see if it can unearth facts sufficient to litigate an indirect infringement claim that did not exist when the complaint was filed.129

The defendants pointed out that “[u]nder parallel facts, this Court in Proxyconn dismissed the plaintiff’s indirect infringement claims with prejudice.”130 The court agreed, stating “[i]nsofar as Plaintiff alleges knowledge of the Patents in Suit based on the filing of the original Complaint in this lawsuit, the holding in Proxyconn controls and Plaintiff has not pled sufficient facts to state a plausible claim for indirect patent infringement.”131

126 Id. (citing Brandywine Commc’ns Techs., LLC v. T-Mobile USA, Inc., 904 F. Supp. 2d 1260 (M.D. Fla. 2012)) (citations omitted).
127 Id.
130 Id. at 6.
Brandywine Communications Technologies, LLC v. Casio Computer Co. Ltd. is the second 2012 decision in the Middle District of Florida dealing with patent infringement claims brought by Brandywine. Indeed, the case also involved a patent for a “Simultaneous Voice/Data Answering Machine,” and was also presided over by District Judge Honeywell. Casio filed a motion to dismiss for lack of pre-suit knowledge of the patent. The court stated that “[t]he weight of authority addressing the knowledge required for indirect infringement, especially following the Supreme Court’s decision in Global–Tech, requires a plaintiff to allege that defendant had pre-suit knowledge of the patents-in-suit.” The court dismissed the indirect infringement claims, concluding “Brandywine cannot avoid the pre-suit knowledge requirement by relying on either the Original Action or letters sent to Casio during the lawsuit, when the parties were already disputing Casio’s alleged infringement.”

### III. Why Federal Circuit Review Is Necessary

The Proxyconn decision from the Central District of California offered the most thorough explanation of the reasoning behind the position that pre-suit knowledge is required to maintain an indirect infringement claim. The decision provides three rationales for granting the defendants’ motion to dismiss. First, it decried what it described as “bootstrapping” post-complaint knowledge to pre-complaint acts by the defendant. Second, it concluded that requiring pre-suit knowledge furthers judicial economy. Third, the court found persuasive that if a defendant continues its actions after the serving of the complaint, the plaintiff can always file a new complaint or amend the original complaint.

---

133 Id. at 1339.
134 Id. at 1345.
135 Id.
136 Id. at 1346.
138 Id. at *5-7.
139 Id. at *5.
140 Id.
141 Id. at *6.
Each of these arguments has visceral appeal. Indeed, it seems highly peculiar that a plaintiff could properly allege the concurrence of both infringing activities and knowledge of the infringed patent in a complaint when the plaintiff (1) knows that knowledge of the patent will not occur until after the defendant reads the complaint and (2) assumes that the defendant will continue to induce or contribute to infringement after gaining knowledge of the patent.

Conversely, courts following the opposite view are quick to point out that the “bootstrap” problem is no problem at all because the “plaintiff would be prohibited from collecting damages related to indirect infringement for any pre-knowledge (e.g., pre-filing) conduct.” In other words, courts finding post-suit knowledge sufficient hold that a defendant is only liable for conduct that occurs after the defendant learns of the patent and the infringing activity. As far as these courts are concerned, “bootstrapping” would only be a concern if courts were to hold that a defendant could be liable for pre-suit conduct based solely on post-suit knowledge. However, no district court offers that view, and such a view would be in stark contrast to the Supreme Court’s holdings in Aro II and Global-Tech.

For its second rationale, the Proxyconn court explained that requiring pre-suit knowledge “furthers judicial economy and preserves parties’ resources by encouraging resolution prior to filing a lawsuit.” Explaining this view, the Proxyconn court stated “[p]re-litigation attempts at resolution are especially desirable in patent cases, which are often expensive and thus resolved by settlement[,]” and that “Plaintiff could have notified Defendants of their alleged infringement and sought an amicable resolution at any time prior to filing th[e] suit[,]” and the defendants “should not be punished for Plaintiff’s failure to do so.”

Along these same lines, the Proxyconn court disagreed with the rationale that “the interests of judicial economy favor denying a motion to dismiss because by the time the motion to dismiss has been filed, defendant in fact has the requisite knowledge,” explaining this view “gives too little weight to the judicial inefficiencies and parties’ expenses in litigating potentially meritless claims.” The court exemplified the propriety of this view by stating that the unfortunate defendant that quit all infringing action the day he received the

---

144 Id.
145 Id. at *7 (internal marks omitted).
complaint would still have to expend vast resources to come to the summary judgment stage of a litigation if post-suit knowledge were sufficient to survive a motion to dismiss.\textsuperscript{146}

However, the courts that disagree with the \textit{Proxyconn} view claim that judicial economy actually favors denying a motion to dismiss because the defendant in fact has the requisite knowledge by the time the motion to dismiss has been filed, despite the fact that \textit{Proxyconn} held that this view “gives too little weight to the judicial inefficiencies and parties’ expenses in litigating potentially meritless claims.”\textsuperscript{147}

For its third and final rationale, the \textit{Proxyconn} court found persuasive that, if a defendant continues its actions after the serving of the complaint, the plaintiff can always file a new complaint or amend the original complaint.\textsuperscript{148} The court explained “nothing prevents a plaintiff from filing a new lawsuit alleging that the knowledge requirement is established because the Defendant is aware of the previous lawsuit . . . [and] Federal Rule of Civil Procedure 15(d) provides a procedure for pleading post-suit facts.”\textsuperscript{149} However, courts holding the contrary view find persuasive that a plaintiff can always amend their complaint by rule to provide factual allegations demonstrating that the knowledge element is met, along with post-knowledge conduct.\textsuperscript{150}

This divide of opinions demonstrates the importance of appellate review of this topic. The complexity of this issue is further underscored by the fact that Judge Robinson switched her stance on the issue in \textit{Walker Digital, LLC v. Facebook, Inc.}\textsuperscript{151} and \textit{Apeldyn Corp. v. Sony Corp.}\textsuperscript{152} after penning one of the seminal cases requiring pre-suit knowledge by the defendant, \textit{Xpoint Technologies, Inc. v. Microsoft Corp.}\textsuperscript{153}

\textbf{IV. CONCLUSION}

The Supreme Court’s \textit{Global-Tech} decision made clear that both forms of indirect infringement require that the defendant have

\begin{itemize}
  \item \textsuperscript{146} \textit{Id.}
  \item \textsuperscript{147} \textit{Id.}
  \item \textsuperscript{148} See \textit{id.} at *6.
  \item \textsuperscript{149} \textit{Id.}
  \item \textsuperscript{150} Rembrandt Soc. Media, LP v. Facebook, Inc., 950 F. Supp. 2d 876, 882 (E.D. Va. 2013).
  \item \textsuperscript{151} See \textit{Walker Digital, LLC v. Facebook, Inc.}, 852 F. Supp. 2d 559 (D. Del. 2012).
  \item \textsuperscript{152} See \textit{Apeldyn Corp. v. Sony Corp.}, 852 F. Supp. 2d 568 (D. Del. 2012).
  \item \textsuperscript{153} See \textit{Xpoint Techs., Inc. v. Microsoft Corp.}, 730 F. Supp. 2d 349 (D. Del. 2010).
\end{itemize}
knowledge of the underlying patent. However, the *Global-Tech* decision also left open the important question of *when* the defendant must have knowledge of the patent. This question remains a highly contentious and heavily divided issue among the district courts, and the divide is only growing. Both camps have well-reasoned explanations for the propriety of their view and appear to have dug in their heels. Thus, Federal Circuit review is necessary in order to resolve the question of whether pre-suit knowledge is necessary in order to maintain a claim for indirect patent infringement.
THE ROLE OF CORPORATE INTEGRITY AGREEMENTS IN THE EXPANSION OF FIDUCIARY DUTIES

Wulf A. Kaal and Elizabeth R. Malay†

I. INTRODUCTION ................................................................. 442
II. EXPANDING FIDUCIARY DUTIES ........................................ 445
III. CORPORATE INTEGRITY AGREEMENTS ............................ 448
    A. BACKGROUND .................................................................. 448
    B. CHARACTERISTICS ......................................................... 450
    C. REACH AND SCOPE........................................................ 451
IV. THE ROLE OF CIAs IN EXPANDING FIDUCIARY DUTIES ......... 454
    A. CONTRACTUAL ADDENDUM TO INCREASE DUTIES 455
    B. DELINEATING THE ROLE OF CIAs IN FIDUCIARY DUTIES .... 456
    C. LIMITATIONS ................................................................. 461
V. CONCLUSION ........................................................................ 463

ABSTRACT

Academics have long debated the purpose and scope of fiduciary duties. The academic debate has mostly ignored the role of Corporate Integrity Agreements (CIAs). CIAs can blur the line between the law and aspirational governance. As a contractual arrangement, the terms of CIAs between health care companies and the government require heightened compliance duties. Unlike regular contractual arrangements, however, the enforcement of CIAs goes beyond contractual remedies. The breach of a CIA can be treated like

† Wulf A. Kaal is an Associate Professor, University of St. Thomas School of Law (Minneapolis) and wishes to thank research librarians Valerie Aggerbeck and Megan McNevin for their outstanding support. Elizabeth R. Malay holds a J.D. 2013, University of St. Thomas School of Law, is an Associate at Winthrop & Weinstine, P.A., Minneapolis, and worked in medical sales for seven years at Alcon Laboratories, Inc.
a breach of law for purposes of the duty of care.

Courts are increasingly recognizing the role of CIAs and their implications for directors’ fiduciary duties. A prominent recent decision, In re Pfizer,1 illustrates the role of CIAs in the evolution of fiduciary duties. Although the court in Pfizer did not conclude that the CIAs actually created fiduciary duties, the court opined that the CIAs “imposed affirmative obligations on Pfizer's board that went well beyond the basic fiduciary duties required by Delaware law.”2 A broader reading of this phraseology suggests that fiduciary duties could perhaps be augmented by contractual arrangements such as CIAs. It seems possible that future courts, in following this reasoning, may interpret CIAs as expanding the basic legal duty of care.

---

2 Id. at 461.
I. INTRODUCTION

Traditional fiduciary duty doctrine is among the most amorphous concepts in the law and leads to confusion, inconsistency, and to cases with somewhat problematic outcomes. The standard for liability is so high that it is hard for courts to find directors in violation of their fiduciary duties. Only a board’s sustained or systematic failure to exercise oversight can result in liability. Academics have debated ways to improve the fiduciary duty doctrine for decades. There is some agreement that fiduciary duties are too vague and should be better defined. Despite various nuances on side issues, the main

3 Claire A. Hill & Brett H. McDonnell, Disney, Good Faith, and Structural Bias, 32 J. CORP. L. 833, 850 (2007) (discussing the various Disney cases).
4 Id. at 846.
5 Lyman P.Q. Johnson & Mark A. Sides, Sarbanes-Oxley Act and Fiduciary Duties, 30 WM. MITCHELL L. REV. 1149, 1198 (2004); see also In re Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996).
6 See, e.g., Claire A. Hill & Brett H. McDonnell, Fiduciary Duties and Emerging Jurisprudence, in RESEARCH HANDBOOK ON THE ECONOMICS OF CORPORATE LAW 133 (Claire A. Hill & Brett H. McDonnell eds., 2012) [hereinafter Fiduciary Duties]; Johnson & Sides, supra note 5, at 1194 (“[I]n corporate law, the duties are broad and usefully ill-defined—decision-makers must act with ‘loyalty’ and ‘care’ and in ‘good faith,’ but are accorded wide latitude in discharging their governance responsibilities in conformance with these standards.”); Cheryl L. Wade, Fiduciary Duty and the Public Interest, 91 B.U. L. REV. 1191, 1192 (2011) (citing TAMAR FRANKEL, FIDUCIARY LAW 166 (2011)) (“[W]hen the public interest conflicts with shareholder primacy and wealth-maximization goals, courts may enforce duties that fiduciaries owe shareholders rather than enforce fiduciaries' compliance with law and regulation that protect the public interest.”); Thomas J. Moloney, Paul R. St. Lawrence III, & Angela F. Hamarich, Fiduciary Duties, Broker-Dealers and Sophisticated Clients: A Mis-Match that Could Only Be Made in Washington, 3 J. SEC. L. REG. & COMPLIANCE 336 (2010) (providing an overview of the fiduciary duty debate); Lisa M. Fairfax, Spare the Rod, Spoil the Director – Revitalizing Directors’ Fiduciary Duty through Legal Liability, 42 HOUS. L. REV. 393, 395 (2005) (“[L]egal liability represents an essential mechanism for ensuring directors' fidelity to their fiduciary duties and for questioning reform efforts that do not include such liability.”); Margaret M. Blair, Stakeholders as Shareholders, Ownership and Control: Rethinking Corporate Governance for the Twenty-First Century, 109 HARV. L. REV. 1150 (1996).
8 One group of scholars emphasizes the differences between the duties of corporate officers and directors. See e.g., Paul E. McGreal, Corporate Compliance Survey, 64 BUS. LAW. 253, 273 (2008) (“Some commentators, taking their cue from agency law, have suggested that an officer’s fiduciary duties should be more demanding [than a director’s].”) (citing Lyman P.Q. Johnson & Robert V. Ricca, (Not) Advising Corporate Officers About Fiduciary Duties, 42 WAKE FOREST L. continuing . . .
debate focuses on whether improvements to the fiduciary duty
document can be attained through expansion or curtailment of the
document.

The academic debate on options for improvement of the fiduciary
duty doctrine has ignored the possible role of Corporate Integrity
Agreements (CIAs). CIAs are administratively-enforced compliance
programs funded by health care companies but enforced by the
government. In other words, they are contracts between health care
companies and the federal government and can involve costly
mandatory compliance measures and penalties. Because the
directors contractually agree to increase compliance by way of an open
door policy with the government, CIAs can substantially increase the
risk of liability for companies whose directors do not act in accordance

---

See generally GREG LUCE, HEALTH CARE LITIGATION
STRATEGIES: LEADING
LAWYERS ON ANALYZING RECENT HEALTH CARE
LITIGATION TRENDS, DEVELOPING
SUCCESSFUL CASE STRATEGIES, AND PROTECTING
CLIENT RIGHTS, DEFENDING THE
HEALTH CARE INDUSTRY AGAINST THE
GOVERNMENT’S EXPANDING AND NOVEL
THEORIES OF LIABILITY (2011).

A board that executes a CIA agrees to increased governmental
scrutiny, including, but not limited to, granting permission for government site visits during the
term of the CIA. Corporate Integrity Agreement FAQ, U.S. DEPT.
HEALTH AND
HUMAN SERVS. OFFICE OF INSPECTOR
Corporate Integrity Agreement FAQ] ("The purpose of a site visit is] to verify the entity's
compliance with the terms of its Corporate Integrity Agreement and to provide OIG
with an opportunity to observe an entity's compliance program in practice. The first-
hand observations obtained while on site provide the OIG with a more accurate and
comprehensive assessment of an entity's compliance program. The site visit also
offers the entity the unique, one-on-one opportunity to educate us regarding the
entity's operations. OIG has also found that site visits help foster more effective
communication between the entity and the OIG.")
with their fiduciary responsibilities. While CIAs are outside the traditional legal framework that formally defines fiduciary duties, they fit into the penumbra of extra-legal forces\textsuperscript{13} that help to clarify the expectations for directors.

The contractual obligations in CIAs can enhance directors’ fiduciary duties, expanding the duty of care for directors of health care corporations beyond the legal standard under Caremark\textsuperscript{14} and Ritter.\textsuperscript{15} The duties imposed in a CIA can include, among others: the passing of specific resolutions; appointment of a chief compliance officer (CCO); agreement that the CCO will increase the frequency of reports to the board; board certification of compliance with the CIA; reporting of compliance issues to the relevant authorities; and annual reviews through an independent review organization.\textsuperscript{16}

Courts are increasingly recognizing the role of CIAs and their implications for directors’ fiduciary duties.\textsuperscript{17} A prominent recent decision, In re Pfizer,\textsuperscript{18} illustrates the role of CIAs in the evolution of fiduciary duties. Although the court in Pfizer did not conclude that the CIAs actually created fiduciary duties, the court opined that the CIAs “imposed affirmative obligations on Pfizer's board that went well beyond the basic fiduciary duties required by Delaware law.”\textsuperscript{19} A broad reading of this phraseology suggests that fiduciary duties could perhaps be augmented by contractual arrangements such as CIAs. Should other courts follow this reasoning, fiduciary duties—and more specifically directors’ basic legal duty of care—could over time expand in the CIA context.

This article includes five parts. Part II introduces the academic debate on the scope and expansion of fiduciary duties. Part III explores the main characteristics of CIAs, their reach and scope, and common denominators in executed CIAs. Part IV outlines the role of CIAs in expanding the law of fiduciary duties both as a contractual addendum and as a hybrid form of aspirational corporate governance.

\textsuperscript{13} See Optimal Penumbra, supra note 7, at 334.
\textsuperscript{14} In re Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996).
\textsuperscript{17} See supra Part IV.2.
\textsuperscript{18} In re Pfizer S’holder Derivative Litig., 722 F. Supp. 2d 453, 461 (S.D.N.Y. 2010).
\textsuperscript{19} Id.
The authors delineate the role of CIAs in fiduciary duties by discussing relevant case law. After exploring the benefits of CIAs for the expansion of fiduciary duties, the authors outline possible limitations. Part V concludes the article.

II. EXPANDING FIDUCIARY DUTIES

The law of fiduciary duties has evolved as a result of both judicial decisions (traditional legal holdings as well as non-adjudicatory writings) and traditional equity and standards-based approaches to governance duties. Traditionally, only two fiduciary duties existed, the duties of loyalty and care. But, fiduciary duty law has evolved in the past few decades and fiduciary duties have expanded. Today, courts recognize intermediate standards, particularly the duty of good faith, making directors responsible for a triad of fiduciary duties. In addition to judicial decisions, the recent financial crises and their legislative fallout have played a role in changing the law of fiduciary duties. The Sarbanes-Oxley Act and the Dodd-Frank Act have influenced and shaped fiduciary duties but have not necessarily improved and clarified them.

---

20 Johnson & Sides, supra note 5, at 1151.
22 Id.; see also Optimal Penumbra, supra note 7, at 347, 353 (claiming that despite the evolution of fiduciary duties, the changes as of yet are incomplete and of disputable value, and arguing that because market forces alone cannot create an optimal director mind-set, and courts alone cannot micro-manage businesses, fiduciary duty law can and should be supplemented by extra legal forces).
23 Optimal Penumbra, supra note 7, at 338; see also Hill & McDonnell, supra note 3, at 834, 845 (citing In re Walt Disney Co. Derivative Litig., 906 A.2d 27, 66-67 (Del. 2006)).
24 Hill & McDonnell, supra note 3, at 848.
25 Johnson & Sides, supra note 5, at 1199. Johnson and Sides point out that, rather than assessing whether directors followed specific rules, judges review the manner in which directors acted. This “process” approach allows a “tailored” response to breach of fiduciary duty claims, resulting in incremental changes to fiduciary duty norms over time. Johnson & Sides, supra note 5, at 1194. Because of this “process” approach, Johnson and Sides argue that laws such as Sarbanes-Oxley are incapable of providing a comprehensive, clearly-defined approach to proper governance – fiduciary duties are much more nuanced and norm-driven than the duties required by such statutes. Johnson & Sides, supra note 5. Johnson and Sides agree that federal statutes can breathe new meaning into our understanding of proper oversight or reasonable care. Johnson & Sides, supra note 5, at 1199. For example, the duty of due care requires directors to monitor the corporation and act with appropriate oversight. Johnson & Sides, supra note 5, at 1198. One often overlooked issue is Chancellor Allen’s admonition in Caremark that directors have...
The academic debate on the scope and reach of fiduciary duties has endured for more than three decades. There is some consensus that fiduciary duties are too vague and should be better defined. A minority of scholars prefer a limited application of fiduciary duties, citing as a particular concern the expansion of fiduciary duties via federal law. To avoid confusion and inconsistency in the law of fiduciary duties, these scholars conceptualize fiduciary duties as a type of contract and a duty of unselfishness. This narrower definition of fiduciary duties is rooted in the concept of entrustment; when the

an “obligation to be reasonably informed,” that they must “exercise reasonable oversight,” and that directors must “assure a reasonable information and reporting system” exists. Johnson & Sides, supra note 5 (citing In Re Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 970-71 (Del. Ch. 1996)). What this means is that directors have an obligation to be “reasonably informed,” and what that obligation means will shift as the legislature passes federal laws setting new norms. Johnson & Sides, supra note 5. Further, part of due care requires directors to ensure their corporation’s compliance with various regulatory schemes. Johnson & Sides, supra note 5, at 1199. This duty will also shift as more laws are passed. Johnson & Sides, supra note 5. Johnson and Sides, while arguing that fiduciary duties are not federalized, acknowledge the impact that federal laws have on governance responsibilities, even though the responsibilities are still broad and open to interpretation.

See, e.g., Ribstein, supra note 7, at 899; Optimal Penumbra, supra note 7, at 336; Johnson & Sides, supra note 5, at 1194.

Ribstein, supra note 7, at 900 (arguing for a more precise definition and more limited application of fiduciary duties).

See Roberta Romano, The Sarbanes-Oxley Act and the Making of Quack Corporate Governance, 114 Yale L.J. 1523, 1529 (2005) [hereinafter Quack Corporate Governance]; Stephen M. Bainbridge, Dodd-Frank: Quack Corporate Governance Round II, 95 Minn. L. Rev. 1779 (2011); Roberta Romano, Answering the Wrong Question: The Tenuous Case for Mandatory Corporate Laws, 89 Colum. L. Rev. 1779, 1785 (1989) [hereinafter Answering the Wrong Question] (arguing that corporate governance laws should not be mandatory even before SOX was passed).

Ribstein, supra note 7, at 902.

30 Ribstein, supra note 7, at 899-900 (arguing that a broader view of fiduciary duties has significant limitations and that the strictness of the duty of unselfishness requires a limited scope). In Meinhard v. Salmon, Justice Cardozo famously described fiduciary duties: “Joint adventurers, like copartners, owe to one another, while the enterprise continues, the duty of the finest loyalty. . . . A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior.” Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928). Ribstein found such a strict duty to be “only rarely appropriate in a competitive marketplace,” so therefore only required in relationships where power was entrusted to a non-owner. Ribstein, supra note 7, at 903. Instead of a broad, vague approach to fiduciary duties, Ribstein believed parties should be able to contractually adjust the duties promised and be held to a simple duty of unselfishness in relationships where there is an entrustment of power. Ribstein, supra note 7, at 907.
control of an organization is separated from the ownership of that organization, the fiduciary duty owed by the controllers protects the owners. In these relationships, it would be costly or impracticable for the owner to fully monitor the controller. Hence, fiduciary duties exist to compensate for owners’ inability to fully monitor the controllers.

A substantial part of the literature supports the expansion of fiduciary duties. The leading argument for the expansion of fiduciary duties is that the traditional fiduciary duty doctrine is inconsistent and can result in cases with problematic outcomes. An increasing number of scholars argue that extra-legal forces can further shape and expand corporate law. The law alone may not always require corporate directors to fulfill their fiduciary duty to shareholders, but extra-legal forces can help fill the gaps. Because state fiduciary duty law is permissive rather than regulatory, fiduciary standards can develop from non-legislative sources. The overall umbrella of fiduciary responsibilities is arguably non-binding, more akin to corporate ‘best practices,’ and aspirational in nature, making extra-legal forces a legitimate source that can help shape fiduciary duties. Extra-legal sources include, among others, the advice given by a corporation’s law firm, judicial pronouncements made outside the traditional legal opinion, and influential academic views in today’s corporate governance scholarship. These extra-legal forces can create norms that help guide directors.

31 Ribstein, supra note 7, at 901.
33 Id. at 10.
34 See, e.g., Fiduciary Duties, supra note 6, at 141; Johnson & Sides, supra note 5, at 1151; see also Wade, supra note 6, at 1207; Moloney, St. Lawrence III, & Hamarich, supra note 6, at 337; Fairfax, supra note 6, at 395; Blair, supra note 6; Optimal Penumbra, supra note 7, at 334, 336.
35 Hill & McDonnell, supra note 3, at 850 (discussing the various Disney cases).
36 Optimal Penumbra, supra note 7, at 334, 336.
37 Optimal Penumbra, supra note 7, at 352.
38 Johnson & Sides, supra note 5, at 1192-93.
39 Johnson & Sides, supra note 5, at 1193.
40 Optimal Penumbra, supra note 7, at 357-58.
41 Optimal Penumbra, supra note 7, at 364.
III. CORPORATE INTEGRITY AGREEMENTS

Corporate integrity agreements can have an impact on fiduciary duties and corporate governance. CIAs are administratively-enforced compliance programs funded by health care companies but enforced by the government. CIAs can enhance directors’ fiduciary duties if directors contractually agree to increase compliance for the companies they manage. Through this mechanism, CIAs increase the stakes for companies whose directors do not act in accordance with their fiduciary responsibilities. Enforcement of CIAs can result in costly mandatory compliance measures and penalties.42

The enhanced duties that can be imposed on boards include: appointment of a chief compliance officer (CCO); agreement that the CCO will increase the frequency of reports to the board; board certification of compliance with the CIA; reporting of compliance issues to the relevant authorities; and annual reviews through an independent review organization. CIAs are not part of the legal framework that defines fiduciary duties. However, CIAs are part of the penumbra of extra-legal forces43 that can expand and help clarify the scope of fiduciary duties.

A. Background

CIAs are a relatively new phenomenon. Beginning in the 1990s, the Department of Health and Human Services Office of the Inspector General (OIG) started using CIAs to resolve False Claims Act investigations.44 CIAs have evolved from an informal set of self-disclosure programs into a formalized process,45 requiring the OIG to negotiate CIAs with health care providers and other entities as part of settlements in the context of health care program investigations under false claims statutes.46 In exchange for providers’ agreement to be bound by the CIA’s substantive provisions, the OIG does not exclude the providers from participation in federal health care programs, including Medicare and Medicaid.47 In effect, the OIG uses providers’ participation in federal health care programs, and the revenues generated through participation, as leverage to negotiate substantive

---

42 LUCE, supra note 11.
43 See Optimal Penumbra, supra note 7, at 334.
45 Id. (discussing, specifically, the Defense Industry Initiative).
46 Corporate Integrity Agreements, supra note 16; see also McGreal, supra note 8, at 265.
47 McGreal, supra note 8, at 265.
provisions in CIAs that increase compliance with expected conduct and overall welfare.

The provisions in CIAs are diverse and depend on the specific terms of the settlement. CIAs are generally adjusted to the fact-specific requirements of the individual company and take preexisting compliance programs into account.\(^{48}\) During the term of a CIA, the company that executed the CIA with the government is required to increase compliance functions, including upgrades to the internal compliance structure, increased third-party oversight, and enhanced reporting requirements.\(^{49}\) In effect, a company that executes a CIA agrees to increased government scrutiny including OIG site visits during the term of the CIA.\(^{50}\)

Noncompliance with a CIA carries serious penalties. Upon noncompliance with the terms of a CIA, the OIG can prosecute the company or seek its exclusion from federal health care programs.\(^{51}\) The penalties under CIAs affect the respective entity and individuals who work for the entity. For instance, companies subject to supervision by the Food and Drug Administration (FDA) may not employ individuals who were dismissed for CIA violations as a

---

\(^{48}\) See Corporate Integrity Agreements, supra note 16 (“A comprehensive CIA typically lasts 5 years and includes requirements to: hire a compliance officer/appoint a compliance committee; develop written standards and policies; implement a comprehensive employee training program; retain an independent review organization to conduct annual reviews; establish a confidential disclosure program; restrict employment of ineligible persons; report overpayments, reportable events, and ongoing investigations/legal proceedings; and provide an implementation report and annual reports to OIG on the status of the entity’s compliance activities.”).

\(^{49}\) James N. Czaban, Meeting the Challenge of Increased Enforcement for Food and Drug Industry Clients, in RECENT DEVELOPMENTS IN FOOD AND DRUG LAW 113, 117 (Eddie Fournier, ed., 2012).

\(^{50}\) Corporate Integrity Agreement FAQ, supra note 12 (“[The purpose of a site visit is] to verify the entity’s compliance with the terms of its Corporate Integrity Agreement and to provide OIG with an opportunity to observe an entity’s compliance program in practice. The first-hand observations obtained while on site provide the OIG with a more accurate and comprehensive assessment of an entity’s compliance program. The site visit also offers the entity the unique, one-on-one opportunity to educate us regarding the entity’s operations. OIG has also found that site visits help foster more effective communication between the entity and the OIG.”).

“Covered Person.” The careers of directors and officers in the pharmaceutical industry who were prosecuted in the context of CIA violations can be severely affected.

CIAs can also facilitate the pursuit of increased sanctions against noncompliant companies. Certification requirements in CIAs, which require directors and officers to certify compliance with the CIA’s provisions, can lower procedural and enforcement hurdles. The number of individuals who are required to provide certifications under CIAs has dramatically increased in the past few years and the certification requirements go well beyond the certification requirements for the CCO. With the increased number of individuals certifying compliance with CIA provisions, the potential for false certifications and corresponding liability intensifies.

B. Characteristics

CIAs have several core characteristics that distinguish them from other contractual arrangements between companies and the government. CIAs often become the standard for expected conduct in a civil or criminal trial. CIA certification requirements can be a powerful tool for prosecutors if the government finds that the certifications misstate the corporation’s true compliance. Once a

53 Czaban, supra note 49, at 114.
55 Id. at 172.
56 Id. at 162 (“There is potential for criminal liability under 18 U.S.C. § 1001, making a material false statement to the United States, if the false certifications are made knowingly. There is also potential for False Claims Act liability for false certifications.”); see also Thomas Beimers, Caught by the CIA: Corporate Integrity Agreement Violation is Grounds for False Claims Act Liability, BEYOND HEALTCARE REFORM (Mar. 7, 2012), http://beyondhealthcarereform.com/caught-by-the-cia-corporate-integrity-agreement-violation-is-grounds-for-false-claims-act-liability/ (demonstrating that the 11th Circuit found that false certifications made as part of CIA obligations could form the basis for False Claims Act liability, and discussing U.S. ex rel. Matheny v. Medco Health Solutions, 671 F.3d 1217, 1224 (11th Cir. 2012)).
58 McDermott & Callender, supra note 54, at 162.
CIA has been executed, it is much easier for the government to reopen a case than to pursue a new one. The OIG’s increased scrutiny, the potential for crippling penalties, and the ease of further prosecution can have a substantial impact on the knowledge, monitoring, and management of boards of companies that operate under a CIA.

A CIA increases the stakes for directors choosing to eschew their governance responsibilities. A company operating under a CIA is essentially on parole. CIAs give the government direct access to a health care corporation, facilitating the detection of compliance issues. A corporation that executed a CIA often gives the OIG permission to inspect the company’s compliance documents and conduct on-site inspections to assess its compliance with the CIA. Should the government find problems upon inspection, it can increase the penalties beyond the CIA’s substantive provisions. These penalties include criminal prosecution, fines, additional CIAs, and exclusion from federally funded health care programs. The $2.3 billion Pfizer settlement in 2009 illustrates how significant possible ramifications can be for companies that engage in illegal activities after executing a CIA.

C. Reach and Scope

By imposing stringent and detailed compliance requirements, CIAs can take an active role in the day-to-day compliance functions of corporations. CIAs affect these day-to-day compliance operations by increasing the role of the Chief Compliance Officer (CCO). Should a regulated entity not have a CCO, a CIA typically mandates the appointment of a CCO. The CCO is responsible for implementing

---

59 Czaban, supra note 49, at 3.
60 Czaban, supra note 49, at 3.
61 See Corporate Integrity Agreement FAQ, supra note 12.
63 See LUCE, supra note 11.
66 See, e.g., Pfizer CIA, supra note 52, at 4 (“Prior to the Effective Date, Pfizer continued . . .
the CIA and must generally report directly to the Chief Executive Officer (CEO), not to the General Counsel or Chief Financial Officer (CFO). CCOs under CIAs usually have direct access to the boards of directors. CIAs typically require companies to create or maintain a compliance committee that supports the CCOs in fulfilling the additional obligations and duties imposed by the CIA. The compliance committee is usually chaired by the CCO.

CIAs can include specific provisions prescribing the conduct of the boards of directors. For instance, CIAs can mandate the number of board meetings dedicated to the review of the company’s compliance program. CIAs may even require boards to adopt specific resolutions to certify the company’s compliance with the CIA and appointed a Chief Compliance Officer and Pfizer shall maintain a Chief Compliance Officer during the term of the CIA. The Chief Compliance Officer shall be responsible for developing the requirements set forth in this CIA and with Federal health care program requirements and FDA requirements.”).

Pfizer CIA, supra note 52 (“The Chief Compliance Officer shall be a member of senior management of Pfizer, . . . shall make periodic (at least quarterly) reports regarding compliance matters directly to the [Audit Committee], and shall be authorized to report on such matters to the Audit Committee at any time . . . . The Chief Compliance Officer shall be responsible for monitoring the day-to-day compliance activities engaged in by Pfizer as well as for any reporting obligations created under this CIA.”).


See, e.g., Allergan CIA, supra note 62, at 5.


See, e.g., Allergan CIA, supra note 62, at 6 (“The Board shall meet at least quarterly to review and oversee Allergan’s Compliance Program, including but not limited to evaluating its effectiveness and receiving updates about the activities of the Chief Compliance Officer and other compliance personnel.”).
increase reporting obligations. In effect, these provisions allow the government to contractually determine how and when a board will interact. The certification requirements can lead directors to require more detailed reports from the corporate officers and take a greater role in overseeing the company’s compliance with both the CIA and federal regulations.

In addition to increasing board obligations and duties of the CCO, CIAs can require a number of other compliance measures. Companies operating under a CIA may be required to develop and implement a written code of conduct, often used to define and explain the role of the CCO. A code of conduct implemented under a CIA may merely require the company’s full compliance with federal, state, and local laws, but it can also demand compliance with FDA requirements, or require compliance with voluntary codes. Codes of conduct also list the consequences of noncompliance with the company’s policies and procedures, the federal health care program, or FDA requirements. Codes of conduct should encourage disclosure of compliance issues and protect whistle blowers from retaliation by maintaining the anonymity of disclosures.

Other CIA provisions require companies to self-report compliance issues to the government, notify the government of communications with the FDA, establish a field force monitoring program, monitor

---

72 See, e.g., AstraZeneca CIA, supra note 70, at 6-7 (“[This resolution] shall be signed by each individual member of the Board or the Committee, summarizing its review and oversight of matters relating to AstraZeneca’s compliance with Federal health care program requirements, FDA requirements, and the obligations of this CIA. . . . The CIA goes on set forth the required minimum language to be used in this resolution:] ‘The Board of Directors [or a Committee of the Board] has made a reasonable inquiry into the operations of AstraZeneca LP and AstraZeneca Pharmaceuticals LP’s Compliance Program for the period . . . , including but not limited to evaluating its effectiveness and receiving updates about the activities of its U.S. Compliance Officer and other compliance personnel. Based on its inquiry, the Board [or the Committee] has concluded that, to the best of its knowledge, AstraZeneca LP and AstraZeneca Pharmaceuticals LP have implemented an effective U.S. Compliance Program to meet Federal health care program requirements, FDA requirements, and the obligations of the Corporate Integrity Agreement.’ If the Board cannot certify such a conclusion in the required resolution, it must set forth the reasons why it is unable to do so and the steps it is taking to ensure compliance with the CIA.”).

73 See, e.g., Medtronic CIA, supra note 68, at 6.
74 See, e.g., Pfizer CIA, supra note 52, at 7-8.
75 See, e.g., DePuy CIA, supra note 70, at 4.
76 See, e.g., Allergan CIA, supra note 62, at 8.
77 See, e.g., DePuy CIA, supra note 70, at 4.
78 DePuy CIA, supra note 70, at 5.
79 See, e.g., AstraZeneca CIA, supra note 70, at 9.
non-promotional activities, provide mandatory compliance training and education for employees, upgrade review procedures, increase disclosure programs, define ineligible persons for employment, and report physician payments. 80 All of these additional requirements, especially the self-reporting provisions, require companies to spend additional resources and, at times, alter their day-to-day operations after signing a CIA. 81

IV. THE ROLE OF CIAS IN EXPANDING FIDUCIARY DUTIES

Courts differentiate between the law and aspirational corporate governance. 82 Corporate fiduciary duties and remedies for duty violations are not aspirational goals of ideal corporate governance practices. 83 Aspirational ideas for boards’ corporate governance practices do not define standards of liability. 84 Although CIAs are not laws, they do go beyond aspirational governance standards. CIAs set forth concrete governance rules that expand the fiduciary duties of directors. CIAs clearly define the duties of directors to be informed, exercise oversight, and establish effective reporting systems – requiring a higher standard of care for directors operating under a CIA.

Several characteristics distinguish CIAs from both the fiduciary duties doctrine and from regular contracts. Unlike the traditional fiduciary duties doctrine, CIAs set out mandatory and clearly defined best practices for companies. Unlike private contracts, companies execute CIAs to avoid further prosecution by the government for various health care fraud charges and to avoid being excluded from Medicaid and Medicare. If the government decides a CIA is warranted, the company’s hands are tied if it wants to continue to operate within its industry.

CIAs combine elements of contractual and public enforcement. As a contractual arrangement, the terms of the CIA between the company and the government dictate heightened compliance duties for the company. Unlike regular contractual arrangements, however, the enforcement of CIAs goes beyond contractual remedies. The OIG may enforce CIAs and private rights of action may also come into play. Because of the combination of enforcement mechanisms, CIAs

80 AstraZeneca CIA, supra note 70, at 16-17, 22, 24, 26-27, 31, 37.
82 In re Johnson & Johnson Derivative Litig., 865 F. Supp. 2d 545, 559-60 (D.N.J. 2011).
83 Brehm v. Eisner, 746 A.2d 244, 256 (Del. 2000).
84 Id.; In re Johnson & Johnson, 865 F. Supp. 2d. at 560.
are more than contractual arrangements. Under Delaware law, CIAs may not only be enforced by the OIG, but also by the courts via a derivative suit.\textsuperscript{85}

**A. Contractual Addendum to Increase Duties**

In lieu of a special hybrid category for CIAs, they are first and foremost contracts. As contracts, CIAs can create a contractual addendum to existing legal duties. To the extent that CIAs mandate specific actions in the day-to-day operations of boards of directors, CIAs can expand boards’ duties. For instance, although federal law prohibits off-label marketing of drugs and devices,\textsuperscript{86} boards are consistently held not liable for companies’ illegal marketing efforts.\textsuperscript{87} However, boards that certify compliance with a CIA are certifying that the company is properly monitoring the promotional activities of its sales teams. Through such certifications, CIAs contractually expand the applicable legal standards for boards.

CIAs can contractually expand directors’ duties beyond the Caremark standard and its progeny. Several CIA features suggest that directors are held to a higher standard after a CIA has been executed. Individual CIA provisions can put boards on notice, highlight extra care requirements in specific areas of operation, and enable the directors to increase their knowledge of the corporation’s activities and corresponding compliance requirements, making it easier to carefully and effectively monitor the organization. More specifically, because CIAs often mandate a CCO and dictate how the CCO interacts with the board, CIAs can increase boards’ knowledge and monitoring of the company’s compliance.\textsuperscript{88} If a board possesses such knowledge, it should play a bigger role in ensuring that the company meets federal and state standards. Moreover, CIAs often require boards to pass specific resolutions certifying compliance.\textsuperscript{89} Besides

\textsuperscript{85} *In re* Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 960 (Del. Ch. 1996).


\textsuperscript{88} See, *e.g.*, Pfizer CIA, supra note 52, at 44 (demonstrating that Pfizer had to submit a written Implementation Report that includes a “certification from the Chief Compliance Officer that, to the best of his/her knowledge” Pfizer is posting payment information on its website); see also AstraZeneca CIA, supra note 70, at 5 (AstraZeneca “appointed a U.S. Compliance Officer” to monitor “day-to-day compliance activities.”).

\textsuperscript{89} See, *e.g.*, AstraZeneca CIA, supra note 70, at 6.
increasing boards’ operational knowledge (thus allowing for a more comprehensive approach to governance), CIAs also demand assurances that boards are meeting their fiduciary duties.

CIA provisions can create economic incentives that affect directors’ diligence in exercising their duties. CIAs can have harsh economic consequences for companies. CIAs provide for penalties in cases of noncompliance. Companies agree in their respective CIA to pay penalties for each day of noncompliance with the agreement. Penalties can add up to thousands of dollars per day. Additionally, most federal health law regulations provide for monetary penalties in cases of noncompliance. Because of the required self-reporting, a company operating under a CIA may be required to report violations of the False Claims Act, Sunshine, Stark, AKS, HIPAA, or other federal health laws. Adding the stipulated penalties in CIAs to the monetary penalties under federal health laws, companies that executed CIAs face significant financial ramifications.

B. Delineating the Role of CIAs in Fiduciary Duties

Caremark underscores that a lack of oversight claim “is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win judgment.” Courts dismiss duty of care cases routinely at the pleading stage.

Courts, however, treat companies that executed a CIA differently.

---

90 AstraZeneca CIA, supra note 70, at 6.
91 See AstraZeneca CIA, supra note 70, at 52.
93 A number of recent cases illustrate that courts have not allowed breach of fiduciary duty suits to proceed when plaintiffs did not make demand upon the boards and failed to adequately plead demand futility. See King v. Baldino, 648 F. Supp. 2d 609, 610 (D. Del. 2009) (dismissing the complaint on the basis that plaintiff did not adequately plead demand futility) (quoting Stone ex rel. v. Ritter, 911 A.2d 362, 373 (Del. 2006)) (“With the benefit of hindsight, the plaintiffs’ complaint seeks to equate a bad outcome with bad faith. The lacuna in the plaintiffs’ argument is a failure to recognize that the directors’ good faith exercise of oversight responsibility may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability, or both, as occurred in . . . this very case.”). See also Markewich v. Collins, 622 F. Supp. 2d 802 (D. Minn. 2009) (finding that the complaint did not plead sufficient facts to allow the inference that the directors operated under a “sustained or systematic failure” to exercise oversight) (quoting Desimone v. Barrows, 924 A.2d 908, 940 (Del. Ch. 2007) (“Delaware courts routinely reject the conclusory allegation that because illegal behavior occurred, internal controls must have been deficient, and the board must have known so.”)). In a pre-CIA setting, both the Baldino and the Markewich court did not allow an assumption of director wrongdoing just because improper behavior occurred.
Courts are increasingly recognizing the role of CIAs and their implications for directors’ fiduciary duties. A prominent recent decision, *In re Pfizer Inc.*,\(^{94}\) illustrates the role of CIAs in the evolution of fiduciary duties. Although the court in *Pfizer* did not conclude that the CIAs actually created fiduciary duties, the court opined that the CIAs “imposed affirmative obligations on Pfizer's board that went well beyond the basic fiduciary duties required by Delaware law.”\(^{95}\) A broader reading of this phraseology suggests that fiduciary duties could perhaps be augmented by contractual arrangements such as CIAs. Following this reasoning, it seems possible that future courts could interpret CIAs as expanding the basic legal duty of care.

In a case with fairly egregious facts, the New Jersey District Court dismissed a derivative complaint against the Johnson & Johnson (“J&J”) board for failure to plead demand.\(^ {96}\) Plaintiffs alleged that the J&J directors breached their fiduciary duty “by permitting and fostering a culture of systematic, calculated and widespread legal violations.”\(^ {97}\) No CIA had been executed before the alleged misconduct.\(^ {98}\) Plaintiffs did not make a demand on the board before filing suit.\(^ {99}\) Plaintiffs’ allegations stated that directors should have known about the company’s questionable acts because J&J received FDA warning letters, an FDA report, subpoenas from the state attorney general, *qui tam* complaints, a criminal plea, and a settlement agreement with the Department of Justice.\(^ {100}\) The court looked to *Brehm v. Eisner*\(^ {101}\) to analyze the case, given the “weighty allegations of corporate misconduct and director inaction.”\(^ {102}\) The *Brehm* court described its case as a case concerning whether directors may be held personally liable “for lack of due care in the corporate decision-making process” – not as a case about whether the directors failed to establish and implement “ideal corporate governance practices.”\(^ {103}\) The *Brehm* court stipulated: “the law of corporate fiduciary duties and

---


\(^{95}\) *Id.* at 461.


\(^{97}\) *Id.*

\(^{98}\) *See id.* at 550-52 (stating that these alleged violations ranged from J & J failing to recall products to J & J subsidiaries engaging in off-label marketing campaigns).

\(^{99}\) *Id.* at 549.

\(^{100}\) *Id.* at 550.

\(^{101}\) *Brehm v. Eisner*, 746 A.2d 244 (Del. 2000).

\(^{102}\) *In re Johnson & Johnson*, 865 F. Supp. 2d at 559.

\(^{103}\) *Id.* (quoting *Brehm*, 746 A.2d at 255-56).
remedies for violation of those duties are distinct from the aspirational goals of ideal corporate governance practices,” meaning that “aspirational ideas of good corporate governance practices for boards of directors . . . are not required by the corporation law and do not define standards of liability.” 104 The J&J court explained that it found these words appropriate when the complaint alleged that the J&J board failed to live up to aspirational ideals but failed to allege that the directors acted in bad faith in violation of their fiduciary duties. 105 The court here differentiated between the law and aspirational corporate governance. 106 However, when a company is operating under a CIA, the distinction between the law and aspirational governance is less clear.

The In re Pfizer Inc. derivative suit followed a number of settlement agreements between Pfizer and the Department of Justice, including a 2009 settlement of $2.3 billion, consisting of the largest criminal fine ever imposed in the United States ($1.195 billion) and the largest civil fraud settlement in history against a pharmaceutical company ($1 billion). 107 Following settlement agreements in 2002, 2004, and 2009, Pfizer signed three separate CIAs with the OIG. 108 Plaintiffs alleged that Pfizer’s directors breached their fiduciary duties by causing or consciously disregarding the illegal marketing activities that led in part to the staggering 2009 settlement. 109 Plaintiffs did not issue a demand upon the board of directors. 110 When analyzing whether demand was futile, the court noted that “many of [the] disturbing reports [of noncompliance] were received during the same time that the board was obligated by the 2002 and 2004 CIAs to pay special attention to these very problems.” 111

104 Id. at 559-60 (quoting Brehm, 746 A.2d at 255-56).
105 Id.
106 Id. at 560.
108 Id. at 457.
109 Id.
110 Id. at 458.
111 Id. The court explained: “As illustrated by the sheer size of the 2009 fines, the wrongdoing here alleged was not only pervasive throughout Pfizer but also was committed in the face of the board's repeated promises to closely monitor and prevent such misconduct, as required by the 2002 and 2004 CIAs. These CIAs, which were part of larger settlements approved by the Pfizer board, imposed affirmative obligations on Pfizer's board that went well beyond the basic fiduciary duties required by Delaware law. Among other things, these agreements obligated Pfizer's chief Compliance Officer to report directly to the board the allegations of misconduct here at issue so that the board could deal with them directly, rather than relying on management. There is no reason to believe this reporting requirement continued . . .
This language is significant. The court stipulated that, in the case of a company that executed a CIA, it would allow an assumption that the directors were fully informed, and thus, willing participants in the corporate malfeasance.\textsuperscript{112} For this reason, the court found that the “plaintiffs ha[d] pleaded with sufficient particularity that a majority of directors faced a substantial likelihood of personal liability because they deliberately disregarded reports of the illegal marketing practices eventually resulting in the 2009 settlement.”\textsuperscript{113} In this case, the CIAs became the court’s proof that the directors could very well have breached their fiduciary duties.

The court in \textit{In re Pfizer} cited \textit{In re Abbott Laboratories Derivative Shareholders Litigation}\textsuperscript{114} [hereinafter “Abbott Labs”], a case that perhaps set the stage for the \textit{In re Pfizer} holding. In \textit{Abbott Labs}, the Seventh Circuit reversed the dismissal of a shareholder suit for breach of fiduciary duty for failure to adequately plead demand futility.\textsuperscript{115} In their complaint, Plaintiffs alleged that Abbott directors breached their fiduciary duty when directors were aware of a six-year history of noncompliance with the FDA, yet failed to take corrective action to prevent further problems, leading to a $100 million fine – then the largest penalty ever imposed for FDA violations.\textsuperscript{116} Plaintiffs alleged directors were aware of and should have corrected the problems because Abbott entered into a Voluntary Compliance Plan with the FDA to address areas of noncompliance six years prior to the FDA filing the injunction that led to the $100 million fine.\textsuperscript{117} Plaintiffs argued that demand would have been futile because the board members knew of the continuing noncompliance with the FDA regulations.\textsuperscript{118} Furthermore, they knew that such noncompliance would lead to severe penalties because of the enhanced government oversight facilitated by Abbott’s Voluntary Compliance Program (VCP) with the FDA, yet still ignored the FDA’s repeated warnings and chose not to stop the problematic conduct.\textsuperscript{119} The Seventh Circuit agreed, holding that it was possible the Abbott directors breached their fiduciary duties.

\begin{itemize}
  \item \textsuperscript{112} \textit{Id.} at 461-62.
  \item \textsuperscript{113} \textit{Id.} at 462.
  \item \textsuperscript{114} \textit{In re Abbott Labs. Derivative S’holder Litig.}, 325 F.3d 795 (7th Cir. 2003).
  \item \textsuperscript{115} \textit{Id.} at 811.
  \item \textsuperscript{116} \textit{Id.} at 801-02.
  \item \textsuperscript{117} \textit{Id.} at 800-01.
  \item \textsuperscript{118} \textit{Id.} at 802.
  \item \textsuperscript{119} \textit{Id.}
\end{itemize}
duty. Although the VCP was not a CIA, the Seventh Circuit used it as evidence that the directors knew of and should have stopped noncompliant activities.

To summarize, courts assume that the boards of companies that executed a CIA have more knowledge and can exercise more control and should thus act with a heightened fiduciary duty. Directors are held to a higher standard if the company executed a CIA. The courts in *In re Pfizer* and *Abbott Labs* found that Pfizer’s CIA and Abbott’s VCP increased the boards’ knowledge about compliance issues, and the directors should have increased their monitoring to prevent further violations. Neither court accepted the directors’ arguments that they did not know about the noncompliance, because executing a CIA or CIA-like agreement means directors do know, or should know, about the respective noncompliance issues.

The *Pfizer* and *Abbott Labs* decisions suggest that CIAs and VCPs can change courts’ evaluations of fiduciary duties. Courts assume that boards operating under CIAs have more knowledge and exercise more control. However, it is unclear if corporations with CIAs will be uniformly affected. In light of the *Pfizer* precedent, future courts could hold directors of corporations that executed CIAs to a higher standard and thereby expand their basic legal duty of care if the facts suggest that CIAs provided directors with more knowledge about compliance activities.

---

120 Id. at 809 (“Given the extensive paper trail in *Abbott* concerning the violations and the inferred awareness of the problems, the facts support a reasonable assumption that there was a ‘sustained and systematic failure of the board to exercise oversight,’ in this case intentional in that the directors knew of the violations of law, took no steps in an effort to prevent or remedy the situation, and that failure to take any action for such an inordinate amount of time resulted in substantial corporate losses, establishing a lack of good faith. We find that six years of noncompliance, inspections, 483s, Warning Letters, and notice in the press, all of which then resulted in the largest civil fine ever imposed by the FDA and the destruction and suspension of products which accounted for approximately $250 million in corporate assets, indicate that the directors’ decision to not act was not made in good faith and was contrary to the best interests of the company.”) (citation omitted).
121 Id.
123 *In re Abbott Labs.*, 325 F.3d at 809; *In re Pfizer Inc.*, 722 F. Supp. 2d at 461.
124 See Pfizer CIA, supra note 52, at 4-5 (demonstrating that the Pfizer CIA contains a number of requirements that seem to ensure a well-informed board. First, the CIA requires the Chief Compliance officer to report directly to the Chief Executive Officer of Pfizer and make at least quarterly reports on compliance matters to the Audit Committee of the Board. Second, the CIA requires the Audit Committee to meet at least quarterly to review Pfizer’s Compliance Program, including receiving updates on its effectiveness. And third, the CIA requires the continued . . .
C. Limitations

Several important conceptual and legal distinctions separate the fiduciary duties created under Delaware precedents and the contractual obligations under CIAs. CIAs have so far been predominantly used in the health care industry. Health care companies serve the greater good and their mission goes beyond the mere maximization of shareholder value. Directors acting on behalf of their corporations in the health care industry face unique challenges. Like other directors, directors in the health care industry are required to make

Audit Committee to certify that it has made reasonable inquiries into the Compliance Program and that Pfizer is meeting the obligations of the CIA. With each certification, Pfizer’s directors are promising that they are exercising proper oversight, and acting with adequate knowledge; see also In re Pfizer Inc., 722 F. Supp. 2d at 461 (“[T]here is no reason to believe this reporting requirement was not fully complied with, thus guaranteeing that each member of the board was bombarded with allegations of continuing misconduct of the very kind that the prior settlements looked to the board to prevent.”).


The Medtronic Mission Statement illustrates the idea that a health care corporation can (and should) strive for more than just profits: “To contribute to human welfare by application of biomedical engineering in the research, design, manufacture, and sale of instruments or appliances that alleviate pain, restore health, and extend life. To direct our growth in the areas of biomedical engineering where we display maximum strength and ability; to gather people and facilities that tend to augment these areas; to continuously build on these areas through education and knowledge assimilation; to avoid participation in areas where we cannot make unique and worthy contributions. To strive without reserve for the greatest possible reliability and quality in our products; to be the unsurpassed standard of comparison and to be recognized as a company of dedication, honesty, integrity, and service. To make a fair profit on current operations to meet our obligations, sustain our growth, and reach our goals. To recognize the personal worth of employees by providing an employment framework that allows personal satisfaction in work accomplished, security, advancement opportunity, and means to share in the company's success. To maintain good citizenship as a company.” Our Mission, MEDTRONIC, http://www.medtronic.com/about-medtronic/our-mission/index.htm (last visited Feb. 13, 2014). The directors are an essential part of such mission: “The corporate director . . . is a bedrock of the health care delivery system. The oversight activities provided by the director help form the corporate vision, and at the same time promote an environment of corporate responsibility that protects the mission of the corporation and the health care consumers it serves.” OFFICE OF THE INSPECTOR GEN. OF THE U.S. DEP’T HEALTH AND HUMAN SERVS. & AM. HEALTH LAWYERS ASS’N, CORPORATE RESPONSIBILITY AND CORPORATE COMPLIANCE, AM. HEALTH LAWS. ASSOC. 11, http://www.healthlawyers.org/hlresources/PI/InfoSeries/Documents/OIG_CorpRespCorpCompliance.pdf (last visited Aug. 5, 2013).
well-informed decisions, oversee the business, and ensure that their respective corporations comply with the law. However, the unique features of health care corporations, in combination with a complex array of federal and state health care legislation, create special challenges for directors in the health care industry. Directors of health care corporations need to balance the needs of many stakeholders such as patients, physicians, taxpayers, the government, and shareholders. Even small health care companies may have a global reach and their directors’ decisions can therefore affect a broad array of constituents. Substantial government involvement and responsibility through Medicare and Medicaid may further complicate the administration of health care providers since the taxpaying public is also a stakeholder.

Given the public good or quasi-public good character of the health care industry, the application of CIAs in industries outside of health

127 Id. at 5 (stating that in the health care context, the duty of care arises in either the decision-making function or the oversight function. The decision-making function applies to a particular situation or a specific action. The duty of care principle in the oversight function pertains to the general activity of overseeing the day-to-day functions of the business).


130 The decisions made by health care corporations have real costs for American taxpayers. See Daniel R. Levinson, Preventing Health Care Fraud: New Tools and Approaches to Combat Old Challenges, U.S. DEP’T OF HEALTH & HUMAN SERVS. (Mar. 2, 2011), http://www.hhs.gov/ash/testify/2011/03/t20110302i.html (“For example, in August 2010, Allergan, Inc., agreed to plead guilty to misdemeanor misbranding and paid $600 million (including a $375 million criminal fine and forfeiture and a $225 million civil settlement) to resolve criminal and civil liability arising from the company’s promotion of Botox®. Our investigations found that the company illegally marketed the drug for indications that, during the relevant time periods, had not been approved as safe and effective by the Food and Drug Administration (FDA). These unapproved indications included headache, pain, spasticity and juvenile cerebral palsy. In addition, the settlement resolved allegations that Allergan misled doctors about the safety and efficacy of Botox®, instructed doctors to miscode claims to ensure payment by Government health care programs, and paid kickbacks to doctors.”).

care could be limited. Without broader application in other industries, the impact of CIAs on corporate law may be limited.

V. CONCLUSION

CIAs add an important element to the academic debate on the expansion of fiduciary duties. As a unique hybrid category, CIAs transcend the law of fiduciary duties and aspirational corporate governance. Courts are increasingly recognizing the role of CIAs and their capacity to expand directors’ fiduciary duties. A broad reading of *In re Pfizer* suggests that CIAs can augment fiduciary default duties. Given the characteristics of CIAs and courts’ increasing recognition of CIAs, courts may interpret CIAs and other hybrid forms, such as deferred prosecution agreements, as expanding the basic legal duty of care. More research and empirical work may be needed to explore how CIAs and other hybrid forms may change or expand directors’ obligations.
VALID BUT HARMFUL: WHY CONGRESS SHOULD AMEND THE PATENT ACT TO COMPULSORY LICENSING OF DISEASE GENE PATENTS

Rebecca Echevarria†

I. INTRODUCTION ................................................................. 466

II. BACKGROUND ................................................................. 466
   A. STATUTORY PATENT-ELIGIBILITY ................................. 467
   B. JUDICIALLY-DEFINED EXCLUSIONS TO PATENTABILITY ......................................................... 469
      1. The Machine-or-Transformation Test .................... 470
      2. The Preemption Test ............................................. 472

III. ANALYSIS .................................................................. 474
   A. THE SUPREME COURT PROPERLY VALIDATED DISEASE GENE PATENTS ......................................... 474
      1. The Supreme Court properly held that process claims involving laws of nature are patent-eligible subject matter .................................................................................. 474
      2. The Supreme Court properly held that disease gene patent compositions of matter claims are patent-eligible subject matter ................................................. 476
   B. DISEASE GENE PATENTS ARE CONTRARY TO PUBLIC POLICY BECAUSE THEY ULTIMATELY DO MORE HARM THAN GOOD ......................................................... 478
      1. Disease gene patents do not further progress and innovation ...................................................................... 479

† B.A. Political Science, Biomedical Ethics (2010), Mount Holyoke College; J.D. Candidate (2014), Wake Forest University School of Law; Staff Member, Wake Forest Journal of Business and Intellectual Property Law (2012-14). The Author would like to especially thank Professor Simone Rose for her guidance and Craig Harasimowicz for his unconditional support throughout this process. Additionally, the Author would like to thank the editors and staff members of the Wake Forest Journal of Business and Intellectual Property Law for their many hours of hard work to prepare this Article for publication.
2. Disease gene patents inhibit physicians’ ability to practice medicine .................................................. 481
3. Disease gene patents deny patients access to secondary medical opinions ........................................ 482
C. CONGRESS SHOULD ENACT COMPULSORY LICENSE LEGISLATION FOR DISEASE GENE PATENTS ............... 484
IV. CONCLUSION ....................................................................................................................... 485
I. INTRODUCTION

CancerX is the sole service provider for the diagnostic test for uterine cancer. Using CancerX’s test, Lisa’s doctor diagnoses her with uterine cancer. He recommends that Lisa undergo surgery to remove her uterus and have chemotherapy to rid Lisa of the cancer. Lisa’s insurance will not cover any of the costly treatments and if she chooses to proceed with the treatment, she will be unable to bear children of her own. Because CancerX holds the patent to the only test for uterine cancer, Lisa is unable to get a second medical opinion or test for false positives before making this life-changing decision.

This is a fictional fact pattern, but the issues Lisa’s story presents are very real. After discovering the genes responsible for breast and ovarian cancer, Myriad Genetics holds the patents to the only genetic test for breast and ovarian cancer.\(^1\) In light of recent Supreme Court cases, disease gene patents present novel questions regarding patent-eligible subject matter. This note discusses the likely effects of \textit{Association for Molecular Pathology v. Myriad ("Myriad")} on scientific progress, physicians’ ability to practice medicine, and patient access to second medical opinions. Unlike other publications in this area, this note does not recommend that disease gene patents be invalidated. After discussing patentable subject matter and analyzing the legal trend in disease gene patents, this note posits that the courts have correctly applied patent law to validate disease gene patents, but that without additional regulation, disease gene patents do more harm than good. This note recommends a new framework of compulsory licensing.

II. BACKGROUND

Article I, Section 8, Clause 8 of the United States Constitution grants Congress the authority “[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;” to that end, Congress enacted the federal Patent Act codified in Section 35 of the United States Code.\(^2\) A patent is a government-granted intellectual property right of an inventor “to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States” for a designated period of time in exchange for

\(^{1}\) Ass’n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2112 (2013).

\(^{2}\) U.S. CONST. art. I, § 8, cl. 8.
public disclosure of the invention. The exclusivity of patents is justified by the assumption that they foster scientific progress and technological innovation. Courts have determined that the main underlying goal of patent law is to benefit the public rather than reward the inventor for his or her efforts. Thus, in order for patents to remain justified, they must lead to higher rates of progress and innovation than their alternative.

Patents confer on their owners a limited monopoly right to exclude others from using their inventions for the benefit of society. If an inventor cannot get a patent for his invention, then his idea could simply be taken by others who wish to benefit from his invention without bearing the costs that went into its creation. Proponents of patents argue that this would likely result in fewer inventors, and thus, less progress in “science and useful arts.” The question remains, however, if this theory is accurate. Furthermore, disease gene patents may deny patients access to secondary medical opinions, which may be essential to making well-informed life-changing decisions.

A. Statutory patent-eligibility

The United States Patent and Trademark Office (“PTO”) is the administrative agency responsible for reviewing patent applications in the United States. The PTO lists three types of patents: design patents, plant patents, and utility patents. Design patents are granted for “new, original, and ornamental design[s] for an article of manufacture.” Plant patents are granted for distinctly new varieties

7 Quanta Computer, 553 U.S. at 626.
8 See Torrance, supra note 4, at 132.
9 Id.
11 Id.
of plants that are discovered and then asexually reproduced. Utility patents are granted for the invention or discovery of “any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.”

Section 101 of the Patent Act states that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” In order for an invention to be patent-eligible, an invention must fit within the scope of patentable subject matter codified in 35 U.S.C. § 101, as interpreted by the courts. If a patented invention fits within the scope of §101, sections 102 and 103 then require that a patented invention be novel and non-obvious to someone of ordinary skill in that area of technology. The claims contained in the patent application must also be written with enough specificity to enable one of ordinary skill in the art to duplicate the invention when the patent term expires. If a claimed invention does not fit within the scope of §101, then there is no need to inquire as to any of these other factors.

The PTO guidelines serve as a useful aid for courts deciding whether a given invention fits within the umbrella of patent-eligible subject matter of §101 of the Patent Act, but it is ultimately up to the courts to make that decision. Looking to the plain language, legislative history, and supporting case law, courts must decide what qualifies as patent-eligible under the Patent Act and the IP Clause’s mandate to “promote the Progress of the useful arts.”

As a federal agency, the PTO’s guidelines and decisions are not per se constitutional and recent court trends have caused the PTO to reevaluate how patent examiners determine eligibility of applications that claim processes involving laws of nature and compositions of matter. On July 3 of 2012, the PTO released a thirteen-page memorandum entitled, “2012 Interim Procedure for Subject Matter

---

12 Id.
13 Id.
15 Id.
18 See Rose, supra note 16, at 121 (explaining that it is the role of the courts to interpret a statute’s meaning).
19 Id. at 133.
Eligibility Analysis of Process Claims Involving Laws of Nature.”

The new PTO guidelines set forth a three-part inquiry to help examiners determine patent eligibility: (1) “Is the claimed invention directed to a process . . . or a series of acts or steps?” (2) “Does the claim focus on use of a law of nature, a natural phenomenon, or naturally occurring relation or correlation?” and (3) “Does the claim include additional elements/steps or a combination of elements/steps that integrate the natural principle into the claimed invention such that the natural principle is practically applied, and are sufficient to ensure that the claim amounts to significantly more than the natural principle itself?”, together with “Is it more than a law of nature + the general instruction to simply ‘apply it’?”

If a given process claim passes the first two inquiries, it must pass the third inquiry in order to be patent-eligible.

B. Judicially-defined exclusions to patentability

Patent categories have historically been viewed very broadly, but there are three judicially created exclusions to patentability: “laws of nature, physical phenomena, and abstract ideas” are ineligible for patents. The constitutional mandate to promote progress in the useful arts includes safeguarding the right to reasonable access to basic knowledge. Because laws of nature, physical phenomena, and abstract ideas are considered basic knowledge, the courts have made these absolute bars to patent-eligibility.

Though laws of nature are barred from patent-eligibility, products of nature and applications of laws of nature are not automatically barred from patent-eligibility. Although neither physical phenomena nor laws of nature are patentable, the Supreme Court in Diamond v. Chakrabarty held that products of nature are patent-eligible with additional human engineering making them “markedly different

---

21 Id. at 3.
22 Id.
24 Id.
25 See Rose, supra note 16, at 121 (examining the Constitutional mandate to promote progress).
26 Id.
compositions of nature.”” A mere “discovery of some of the handiwork of nature” is not patent-eligible because information that is “part of the storehouse of knowledge of all men . . . [is] . . . reserved exclusively to none.” To put it differently, laws of nature are not patent-eligible, but process claims involving laws of nature may be patent-eligible.

Like physical phenomena and laws of nature, the Supreme Court in Mayo v. Prometheus held that abstract ideas that do more than simply state the idea are not automatically barred from patent eligibility. “An application of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.” It is not enough to simply state a law and say “now apply it,” but, “a particular, inventive application of the law” may have enough human involvement to make the matter patent-eligible.

There is no clearly defined test that courts must employ to determine whether a given invention is patent-eligible, and as science evolves outside the anticipated scope, it becomes increasingly more difficult for courts to distinguish between patent-eligible and patent-ineligible subject matter. Disease gene patents present such a struggle. The courts have historically relied on two major doctrinal tests for patent-eligibility—the machine-or-transformation test and the preemption test—but modern science often manages to blur the lines of patent-eligible subject matter that these tests attempt to establish.

1. The Machine-or-Transformation Test

When determining whether a given invention or process is patent eligible, the courts have long employed the machine-or-transformation test. The machine-or-transformation test states that a claim is likely patent-eligible when “(1) it is tied to a particular machine or apparatus, or (2) transforms a particular article into a different state or thing.”

27 Chakrabarty, 447 U.S. at 310.
29 Mayo Collaborative Serv. v. Prometheus Lab., Inc., 132 S. Ct. 1289, 1293–94 (2012) (emphasis added) (holding that the mere description of a correlation between thiopurine metabolite levels and toxicity/efficacy of thiopurine drugs was insufficient to make the application patent-eligible because it did not apply the law of nature to a known structure or process. A patent application must do more than simply state a law and say “apply it.”).
30 Id. at 1290.
Although still employed by courts today, the Supreme Court in *In re Bilski* said the machine-or-transformation test “is not the sole test for determining the patent eligibility of a process . . . but rather is a useful and important clue, an investigative tool, for determining whether some claimed inventions are patent-eligible processes.”

The Court in *In re Bilski* noted that the machine-or-transformation test had been created during the Industrial Revolution, a time in which inventions were expressly tethered to machines or other physical forms. In today’s technological age, inventions are not always tethered to a machine or physical transformation and the way in which the courts make their determinations must evolve along with the technologies with which they deal. The Court noted that the machine-or-transformation test does not work for all cases. There may be inventions that satisfy the test but are patent-ineligible, and some that do not satisfy the test but are still patent-eligible.

The machine-or-transformation test ultimately tries to determine whether there is ‘inventiveness’ present in a given invention. As Chief Justice Marshall explained, if the invention results in something that is markedly different from a naturally occurring phenomenon or idea, it will likely be patent-eligible. Building upon this principle, the Court in *In re Bilski* explained that post-solution steps do not contribute to patentability because the core invention still requires inventiveness.

Post-solution steps are insignificant if they do no more than recite a specific machine or a particular transformation of a specific article. An insignificant step, such as data gathering or outputting, is not sufficient to pass the test without further inventiveness.

In *Funk Bros.*, the Supreme Court said a bacteria-mixture patent was not patent-eligible because the interaction of the two species, though useful and novel, was nothing more than a naturally occurring phenomenon. In *Diamond v. Chakrabarty*, however, the Court said a patent claiming a genetically engineered bacterium was patent-eligible because the bacteria in their genetically modified state were unlike any found in nature. By inserting two plasmid coding for hydrocarbon degradation enzymes, Chakrabarty transformed the bacteria into a new composition possessing characteristics “possessed

---

32 Id. at 3221.
33 Id. at 3227.
34 Id.
35 Id.
36 Davis v. Palmer, 7 F.Cas. 154 (C.C.D. Va. 1827).
38 USPTO Guidance Memo, supra note 20, at 5-6.
by no naturally occurring bacteria." The Court found the fact that the engineered bacteria could clean up oil spills and serve a useful purpose irrelevant and relied on the fact that Chakrabarty had "produced a new bacterium with markedly different characteristics from any found in nature" to validate the biopatent.

Diamond v. Chakrabarty marked the first time the Court granted a non-plant patent of a living thing. With the arrival of biotechnology, mankind is now able to manipulate and alter living things, resulting in markedly different products. Researchers can also now adequately explain their processes in enough detail for them to be replicated upon the expiration of the patent term.

Biopatents introduced a new era of patents, but their advent challenged the practicality of the machine-or-transformation test. Courts may still use the machine-or-transformation test as a helpful tool to determine inventiveness, but as the Supreme Court explained in Mayo v. Prometheus, the Court’s inquiry may not stop there. Courts must also ask if a given invention would preempt others from employing fundamental principles that would benefit society.

2. The Preemption Test

Patent claims that may preempt ideas already in "the storehouse of knowledge of all men," including basic tools of science and abstract ideas are not patent-eligible because they prevent future inventions.

---

41 Id. at 310.
43 See Christopher M. Holman, Bilski: Assessing the Impact of a Newly Invigorated Patent-Eligibility Doctrine on the Pharmaceutical Industry and the Future of Personalized Medicine, 10 CURRENT TOPICS IN MED. CHEM. 1937, 1940 (2010) ("[T]he key distinction is human intervention; products and processes arising out of active human invention are patent-eligible . . .").
44 See Duffy, supra note 42, at 630 (explaining a weakness in only using a per se exclusion to patentability for living inventions is that the rule could still be circumvented by claiming a living invention in conjunction with an inanimate carrier material, such as a bacteria on top of a petri dish).
The preemption test goes beyond the machine-or-transformation test and asks whether a patent could prohibit another inventor from employing a fundamental principle that would be necessary for scientific progress.48

Fundamental principles are necessary for other inventors to use when inventing around them would be nearly impossible.49 Congress has tasked the PTO and the courts to ensure that fundamental principles and basic ideas remain freely available to the public for the sake of scientific progress.50

The Bilski Court found that certain claimed methods passed the machine-or-transformation test, but were still not patent-eligible because they encompassed fundamental principles, which, if controlled exclusively, would preempt any future innovation in the field.51 The processes claimed were too broad to invent around and would give patent owners exclusive control over basic ideas.52 Conversely, the Court in Diamond v. Diehr granted a patent for the use of a well-known mathematical formula in a process for curing synthetic rubber because the Court found no preemption issue.53 The patent claimed a formula that contained a fundamental principle, but the patentees “did not seek to pre-empt the use of that equation” and only sought to prevent others from using the equation in conjunction with all of the other steps described in their claim.54 Patent applicants can pass the preemption test by claiming a specific application of a fundamental principle accompanied by additional conditions, rather

49 See Rochelle C Dreyfuss & James P. Evans, From Bilski Back to Benson: Preemption, Inventing Around, and the Case of Genetics Diagnostics, 63 STAN. L. REV. 1349, 1352 (2011) (examining when fundamental principles are necessary to remain in the public domain).
50 See Golden, supra note 46, at 1074 (discussing the role of the PTO in ensuring progress is being pursued).
52 See Bryan Treglia, Patentable Subject Matter: Separating Abstract Ideas and Laws of Nature from Patentable Inventions, 48 JURIMETRICS J. 427, 437 (2008) (discussing how no one should have exclusive control over basic ideas).
53 See Diamond v. Diehr, 450 U.S. 175, 187 (1981) (granting a patent for the use of a well-known mathematical formula because patentees did “not seek to pre-empt the use of that equation,” and only sought to prevent others from using the equation in conjunction with all of the other steps described in their claim.).
54 Id. Unlike in Flook, where the claims to a formula for setting alarm limits were limited in scope such that they did not actually prevent the use of the formula in other applications, in Diehr, the Court said that the limitation of the scope of application was merely “post-solution activity.” Parker v. Flook, 437 U.S. 584, 590 (1978). The courts make it clear that post-solution activities without any inventive step do little to ameliorate preemption concerns.
than the fundamental principle itself.\textsuperscript{55}

\textbf{III. ANALYSIS}

\textbf{A. The Supreme Court properly validated disease gene patents}

Disease gene patents generally encompass both process claims involving laws of nature and the compositions of matter created in order to develop treatments.\textsuperscript{56} Opponents of disease gene patents typically rely on patent law to argue that disease gene patents should be invalidated as unpatentable subject matter under § 101,\textsuperscript{57} but the Supreme Court properly interpreted patent law in validating disease gene patents. The danger of disease gene patents is not the patent themselves, but rather the manner in which they are being enforced.

\textit{1. The Supreme Court properly held that process claims involving laws of nature are patent-eligible subject matter}

On March 20, 2012, the Supreme Court unanimously held in \textit{Mayo v. Prometheus} that the personalized medicine dosing method invented by Prometheus Laboratories (Prometheus) was ineligible for patent protection as a law of nature.\textsuperscript{58} Prometheus is a specialty pharmaceutical and diagnostics company that researched the use of thiopurine drugs in the treatment of certain autoimmune diseases, such as Crohn's disease and ulcerative colitis.\textsuperscript{59} Prometheus filed patents for a diagnostic test that could determine the proper dosage of thiopurine drug for any given patient.\textsuperscript{60} Every individual metabolizes drugs differently and if a dose is too high or too low, there may be adverse side effects and lower efficacy of the drug.\textsuperscript{61} When Prometheus filed for its patents, the exact correlation between metabolites and thiopurine drug efficacy was unknown, but the active metabolites responsible for thiopurine drug efficacy had already

\textsuperscript{55} See id. (explaining that the proper inquiry in preemption is whether a patent preempts the use of a natural phenomenon).


\textsuperscript{59} See id.

\textsuperscript{60} Id. at 1290-91.

\textsuperscript{61} Id.
been identified and were commonly known to researchers.  

Each of Prometheus’s claims recites an “administering” step, a “determining” step, and a “wherein” step. The administering step merely instructs physicians to administer the drug to the patient; the determining step tells physicians to then measure resulting metabolite in the patient’s blood; lastly, the wherein step instructs physicians to decrease or increase the dosage if the metabolites are outside the ideal range. The methods for making these determinations were already well known in the art before Prometheus came along, and the Court said that simply telling doctors to engage in “well-understood, routine, conventional activity previously engaged in by scientists in the field” was insufficient to make a patentable-ineligible law of nature patent-eligible.

As previously discussed, laws of nature are patent-ineligible subject matter, but applications of laws of nature are permissible so long as there is additional human engineering giving them “markedly different characteristics from any found in nature.” The Supreme Court held that the correlation between thiopurine drug efficacy and the prevalence of metabolites in a person’s body is an entirely natural process, thus making Prometheus’s patents invalid for simply putting forth a natural law. The Court reiterated that an application of a law of nature must be limited in scope so as not to broadly preempt use of the law, and include an “inventive concept” that is significant and separate from the natural law itself. A mere statement of a naturally occurring correlation, despite being newly discovered, fails this inquiry. Additionally, “drafting efforts designed to monopolize the correlations” do not satisfy this requirement. The Court invalidated the Prometheus patent but held that process claims could be patent-eligible with an additional inventive step. After Mayo, disease gene patented method claims are clearly patent eligible subject matter so long as they meet this extra step. The Court correctly applied patent law to uphold process claims involving laws of nature and disease gene patents claiming processes involving laws of nature are patent-eligible.

---

62 Id. at 1295.
63 Id. at 1290.
64 Id.
65 Id. at 1291 (citing Parker v. Flook, 437 U.S. 584, 590 (1978)).
67 See Mayo Collaborative Services, 132 S. Ct. at 1291.
68 Id. at 1292.
69 Id.
70 Id. at 1291.
2. The Supreme Court properly held that disease gene patent compositions of matter claims are patent-eligible subject matter

After the Supreme Court’s landmark decision on bioproduct process patents in Mayo, it addressed the patent eligibility of disease gene compositions of matter. Much of the Supreme Court’s reasoning in Mayo paved the way for Myriad. On March 20, 2012, the Supreme Court unanimously invalidated Myriad Genetics’ (“Myriad”) isolated DNA patents as products of nature, but held that Myriad’s synthetically-created DNA, known as complimentary DNA (“cDNA”), is patent-eligible because it does not naturally occur.\(^{71}\)

Unlike the patent holder in Mayo, who claimed a process involving a law of nature, Myriad claimed a process for isolating and creating cDNA and claimed the individual compositions of matter.\(^{72}\) The Federal Circuit had previously held both isolated DNA and cDNA patent-eligible, finding that isolated DNA is chemically distinct from naturally occurring DNA and cDNA is biologically and chemically distinct from its natural form.\(^{73}\) The Supreme Court—largely echoing Federal Circuit Judge Bryson’s dissent—held that isolated DNA is not patent-eligible subject matter much like “snapping a leaf from a tree” is not patentable.\(^{74}\)

Myriad discovered that mutations of BRCA1 and BRCA2 genes “can dramatically increase the risk of breast and ovarian cancer” and marketed the only genetic test for those cancers.\(^{75}\) The PTO granted Myriad patents for its isolated DNA sequences containing the BRCA1/2 mutations, the cDNA synthesized from the mutated genes for further research, and the diagnostic methods of identifying mutations in those DNA sequences.\(^{76}\) When other medical professionals began performing cheaper versions of Myriad’s genetic test, Myriad filed patent infringement suits, but the infringers counterclaimed that Myriad’s patents were invalid.\(^{77}\) After the Supreme Court vacated and remanded the case to the Federal Circuit in light of Mayo, the Federal Circuit held that Myriad’s method claims directed at “comparing” or “analyzing” DNA sequences were patent-

\(^{71}\) Ass’n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2114 (2013).
\(^{73}\) Id. at 1303-04.
\(^{74}\) Id. at 1352.
\(^{75}\) Myriad, 133 S. Ct. at 2109.
\(^{76}\) Id.
\(^{77}\) Id. at 2114.
ineligible because they merely claimed an “abstract mental process” and contained no transformative steps; however, Myriad’s claims over the isolated DNA and cDNA were patent-eligible compositions of matter.\textsuperscript{78} The Supreme Court affirmed in part and reversed in part.\textsuperscript{79} The Supreme Court unanimously agreed that cDNA was patent eligible, but isolated DNA was not.\textsuperscript{80} Isolated DNA is biologically identical to naturally occurring DNA; the nucleotide sequence found in isolated DNA, which in turn codes for the proteins that make up the BRCA1/2 genes, appears identically in isolated DNA as it does in naturally occurring DNA.\textsuperscript{81} In order to isolate the relevant DNA sequence, Myriad breaks the chemical bonds holding the DNA sequence to the rest of a subject’s DNA.\textsuperscript{82} The Federal Circuit concluded that this chemical difference was sufficiently transformative to qualify isolated DNA as a composition of nature, but the Supreme disagreed. Unlike isolated DNA, cDNA is artificially synthesized through the splicing of genetic material and is both chemically and biologically different than naturally occurring DNA.\textsuperscript{83} The cDNA is synthesized from mRNA after transcription, in which non-coding intron sequences are naturally cut out.\textsuperscript{84} DNA does not naturally exist in the nucleotide sequence formed in cDNA and is thus biologically distinct from naturally occurring DNA.\textsuperscript{85} Additionally, the chemical bonds joining the nucleotide sequences have to be broken and remade in order to bind the new nucleotide sequence together, also making cDNA chemically distinct from naturally occurring DNA.\textsuperscript{86} The Court unanimously held cDNA to be patent-eligible as a composition of matter that “is not a ‘product of nature’” due to human intervention.\textsuperscript{87} Unlike cDNA, isolated DNA retains the same nucleotide sequence as naturally occurring DNA.\textsuperscript{88} In order to isolate the DNA sequences, the chemical bonds of the DNA must be broken through human intervention, making it a chemically distinct molecule from naturally occurring DNA, but the isolated DNA retains the same biological

\textsuperscript{78} Ass’n for Molecular Pathology v. U.S. Patent & Trademark Office, 689 F.3d 1303, 1333 (Fed. Cir. 2012).
\textsuperscript{79} Myriad, 133 S. Ct. at 2111.
\textsuperscript{80} Id.
\textsuperscript{81} Id. at 2116.
\textsuperscript{82} Id. at 2117.
\textsuperscript{83} Id. at 2119.
\textsuperscript{84} Id. at 2112.
\textsuperscript{85} Id. at 2119.
\textsuperscript{86} Id.
\textsuperscript{87} Id.
\textsuperscript{88} Id.
identity. The Federal Circuit held that this chemical distinction was sufficient to render isolated DNA patent-eligible because “genes are in fact materials having a chemical nature and, as such, are best described in patents by their structures rather than by their functions.” In his dissent, Judge Bryson opined that, “merely isolating the products of nature by extracting them from their natural location and making those alterations that are attendant to their extraction does not give the extractor the right to patent the products themselves.” The Supreme Court agreed with Judge Bryson’s reasoning and held isolated DNA patent-ineligible. The utility of isolated DNA is its nucleotide sequence, which codes for a targeted gene, like BRCA1/2.

The Supreme Court was correct to validate Myriad’s cDNA patents and the resulting diagnostic gene test for breast and ovarian cancer. The Supreme Court also properly refused to address the public policy harms of Myriad’s patents and narrowed their inquiry to whether the claimed inventions were patent-eligible subject matter. Disease gene patents cannot be invalidated because of their potential harms to medical consumers when existing patent law certifies their validity.

B. Disease Gene Patents are contrary to public policy because they ultimately do more harm than good

The Supreme Court correctly applied all doctrinal tests, but the “correct” holding may have profound negative consequences. As previously discussed, patent law derives from the constitutional mandate for Congress “[t]o promote the Progress of Science and useful Arts . . .” Patent law arguably only remains valid so long as it continues to promote the progress of science and useful arts. If disease gene patents do not further innovation and science and do more harm than good, then it is time for Congress to enact new legislation to remedy this result.

89 Id.
91 Id. at 1350.
92 See Rose, supra note 16, at 131–32.
93 U.S. CONST. art. I, § 8, cl. 8.
1. Disease gene patents do not further progress and innovation

Recent studies reveal that there is little evidence showing that patents do, in fact, further innovation and scientific progress and suggest that the opposite may be true. Patents slow research by “impeding others from expanding on or improving a [patented] diagnostic test.” Not only can patentees prevent laboratories and physicians from using a patent-protected test to diagnose a patient or verify result, but they may also “block development of variations” of the test. “This precludes researchers from using verification testing to identify false positives or negatives in an extant test,” or from using the patented test on alternative DNA samples. Follow-on research on patented gene patents is done to a much lesser extent than on other types of follow-on research.

Several studies attempting to analyze the correlations between innovation and patent protection have shown that in certain scenarios, patents slow down innovation rather than help speed it up. These studies generally take two forms: 1) the first relies on economic frameworks to determine if patents promote innovation, and thus increased amounts of new technologies are hitting the market; 2) the second employs mathematical models which either measure technological innovation in a single economy of interest or compare rates of technological innovation among countries offering different levels of patent protection.

In Helsinki, Finland, a group of economists using the first model of patent efficacy studies determined that, “while the effect of patents

94 See Torrance, supra note 4, at 135.
95 Katherine L. Record, University Opposition to Unfettered Research: A New Bedfellow for Biotech?, 22 HEALTH MATRIX 139, 150 (2012).
96 Id.
97 Record, supra note 95 at 150.
99 Record, supra note 95, at 151 (quoting DEPT OF HEALTH & HUMAN SERV'S, SEC'Y'S ADVISORY COMM. ON GENETICS, HEALTH, AND SOC'Y, GENE PATENTS & LICENSING PRACTICES & THEIR IMPACT ON PATIENT ACCESS TO GENETIC TESTS 4 (2010) (patent ownership “fragmentation is ... problematic for follow-on contributors to the public knowledge stream [and] ... the negative effect of patents on follow-on public knowledge production is greatest for genes closely linked to human disease”).
100 See Torrance, supra note 4, at 138.
101 Id. at 139.
is to raise the rents on and thereby the potential amount of innovations, it also tends to slow down market introduction."\textsuperscript{102} Similarly, an empirical study done at Columbia University School of Law supported the same finding.\textsuperscript{103} In order to test the hypothesis that patent systems promote innovation in the United States, Dr. Andrew W. Torrance and Dr. Bill Tomlinson created a program to simulate the behavior of inventors and competitors experimentally in both patent and non-patent systems.\textsuperscript{104} The study employed a multi-user interactive simulation of patent and non-patent systems called, “PatentSim”\textsuperscript{105}. Following a model of the invention process, PatentSim allowed law students to access a database of potential innovations, then patent, or open source these innovations. Users could then license, assign, buy, infringe, or enforce patents against each other. The results of the simulation suggest that a system “combining patent and open source protection for inventions (that is, similar to modern patent systems) generates significantly lower rates of innovation” than non-patent systems.\textsuperscript{106}

In 2003, the National Academies published one of the most comprehensive reviews of the United States patent system, entitled “Patents in the Knowledge-Based Economy”.\textsuperscript{107} Instead of supporting the hypothesis that patents spur invention and innovation, the National Academies concluded that “[t]here are theoretical as well as empirical reasons to question whether patent rights advance innovation in a substantial way in most industries.”\textsuperscript{108} Firstly, the benefits of retaining a patent monopoly for a limited time might be outweighed by the ultimate cost of detailed disclosure that patents require.\textsuperscript{109} Secondly, while technological advances are, more often than not, built cumulatively upon other inventions, broad patent protection on upstream discoveries impedes subsequent innovations.\textsuperscript{110} In an empirical study surveying fifty-three biotechnology companies in Switzerland, a group of researchers concluded that a broad research

\textsuperscript{102} Tuomas Takalo & Vesa Kanniainen, Do Patents Slow Down Technological Progress?: Real Options in Research, Patenting, and Market Introduction, 18 INT’L J. OF INDUS. ORG. 1105, 1105 (2000).

\textsuperscript{103} See Torrance, supra note 4, at 138.

\textsuperscript{104} See generally Torrance, supra note 4.

\textsuperscript{105} Id.

\textsuperscript{106} Id.

\textsuperscript{107} Id.

\textsuperscript{108} NAT’L RESEARCH COUNCIL, PATENTS IN THE KNOWLEDGE-BASED ECONOMY 2 (Wesley M. Cohen & Stephen A. Merrill eds., 2003) [hereinafter NAT’L RESEARCH COUNCIL].

\textsuperscript{109} Id.

\textsuperscript{110} Id.
exemption from patent protection, combined with compulsory licensing arrangements for DNA patents are feasible remedies for overcoming the stifling effect the current patent system can often have.\footnote{Nikolaus Thumm, Patents for Genetic Inventions: A Tool to Promote Technological Advance or a Limitation for Upstream Inventions?, 25 TECHNOVATION 1410, 1410 (2005), available at http://www.sciencedirect.com/science/article/pii/S0166497204001154.}

The current patent system arguably does not further progress, and, at the very least, it is questionable. If the patent system is only valid so long as it furthers progress, then it may be time for Congress to reassess whether the current patent regime is still constitutionally valid. Furthermore, any possible value patents provide must also be weighed against their potential harms. Particularly with regard to disease gene patents, limiting patients’ access to secondary medical opinions and affordable drugs and treatments may ultimately be against public policy.

2. *Disease gene patents inhibit physicians’ ability to practice medicine*

Disease Gene patents may materially inhibit physicians’ ability to practice medicine and provide medical care to their patients. The United States, like most of the world, has long recognized the dangers of monopolies and the public harm that may arise when one company retains exclusive control of a market. These dangers are exponentially increased when they occur in medical diagnostic testing. Disease gene patents deserve special attention because of the special way they affect medicine. They not only affect the available treatments that a doctor may proscribe, but they also affect a physician’s ability to practice medicine by performing the patented tests. This trouble does not arise from the patent itself but from patent owners refusing to license their diagnostic tests.

Proponents of disease gene patents argue that without patents, such discoveries would be held as trade secrets, denying patients access to diagnostic tests indefinitely. Secrecy, however, is contrary to the goals of the entire field of sciences and “is particularly disgraceful in the health sciences.”\footnote{Jon F. Merz, Disease Gene Patents: Overcoming Unethical Constraints on Clinical Laboratory Medicine, 45 CLINICAL CHEMISTRY 324, 325 (1999), available at http://www.clinchem.org/content/45/3/324.long#ref-10.} Furthermore, researchers with ordinary skills in the art can typically replicate a diagnostic test once identified in its simplest terms without any further development.\footnote{Id.} Identification of
the genetic loci for a disease trait is typically enough information for one of ordinary skill in the art to develop a similar diagnostic test, and trade secret law would do little to prevent their downstream development.\footnote{Id.}

Patent holders/exclusive licensees can monopolize an entire medical service. Furthermore, disease gene patents can potentially inequitably extend the term of a gene patent. Like BRCA1/2, several genes are often responsible for a particular disease. Patent law foresees that after a gene patent’s term ends, the diagnostic test would become public domain; however, future discoveries and patents on additional genes responsible for the same disease would effectively extend the life of the patent on the diagnostic test. The ability to test for breast cancer would no longer merely require testing for the originally patented mutations in BRCA1 and BRCA2, but would essentially require testing for the additional mutation responsible for the disease. The disease gene patent would then run until the term of the latest patent expired, extending the intended period of patentability. Exclusive disease service providers will interfere with the practice of medicine because they will have the “ability to prescribe nationwide medical practices and to dictate the medical standard of care.”\footnote{Id.} Patents restrict the types of tests physicians and clinicians may perform and the conditions for which they may be done.\footnote{Id.}

3. \textit{Disease gene patents deny patients access to secondary medical opinions}

Disease gene patents are particularly concerning because they may deny patients access to secondary medical opinions. Courts have consistently recognized a patient’s right to a second medical opinion as a matter of public policy.\footnote{Rush Prudential HMO, Inc. v. Moran, 536 U.S. 355, 400 (2002).} There is often more than one way to approach any set of medical facts, and doctors may misdiagnose a condition.\footnote{Renee Bacher, \textit{Half of Americans Don’t Get a Second Opinion}, NBCNEWS.COM, http://www.nbcnews.com/id/22829371/ns/health-health_care/t/half-americans-dont-get-second-opinion/ (last updated Feb. 4, 2008).} Most doctors and insurance plans, including Medicare, frequently require that patients receive a second medical opinion.
before having nonemergency surgeries and treatments. In *Rush Prudential HMO, Inc., v. Moran*, the Supreme Court upheld laws in 42 states that give patients a right to a second medical opinion from outside doctors if their HMOs turn them down for a medical treatment or a drug benefit. Both patients and insurers have an interest in obtaining second opinions because they help to guard against unnecessary surgeries and treatments that may be costly and life-changing. When the federal government recognized these benefits, Medicare became the first indemnity insurance plan to pay for beneficiaries to receive second medical opinions. By the mid-1980s, “second opinions were a well-established feature” of almost all other indemnity insurance programs in the United States. In 1986, the federal government considered “making second opinions mandatory for all Medicaid recipients for ten common elective surgical procedures” but the government considered second medical opinions a patient’s right, rather than a burden.

Today, patients do not seek second opinions as often as they did in the 1980’s. The current American healthcare system has moved away from indemnity insurance and fee-for-service medical care to integrated systems of coverage and care, which shift financial risk to providers; however, for procedures that insurance may not cover—i.e., expensive cancer treatments—doctors often still recommend that patients seek a second medical opinion. Even if most second

---


125 See *Hyman, supra* note 123, at 1457.

126 *Id.*

opinions just confirm what a patient’s original physician recommended, they still play an important role because they offer patients peace of mind before they have to make life-changing decisions. In the instances in which primary physicians misdiagnose patients, second opinions can have profound economic and physical effects.

C. Congress should enact compulsory license legislation for disease gene patents

Some proponents of change call for Congress to broaden the experimental use exemption currently available to academic researchers to make gene sequences freely available to those in research, but this does not remedy all of the public harms of disease patents. While this would allow biomedical research taking place at nonprofit academic research laboratories to openly infringe gene patents, it would not allow any of those to make their way to the market to benefit consumers. Patients like Lisa would still be unable to get a second medical opinion or check for false positives.

Compulsory licensing would not undermine the intended purpose of patent protection. As previously discussed, patents grant inventors negative rights in their inventions so that they may recoup costs and profit from their development, so as to incentivize the innovation. Patentees can still recoup costs and profits if they were federally compelled to license their patented disease gene sequence in exchange for a statutory set fee. The licensing fee could be “tied to the commercial value of the product developed as a result of the licensee’s research.” Compulsory licensing of disease gene patents would ensure that available tests be improved upon and allow physicians to practice medicine by using the patented inventions to give secondary diagnoses and treatment options.

This would not be the first time Congress has acted to protect the interests of medical consumers. In 1984, Congress acted to safeguard consumer access to healthcare by enacting the "Drug Price Competition and Patent Term Restoration Act of 1984”—also known as the Hatch-Waxman Act—which established the Annotated New

---

130 Id.
Drug Application process ("ANDA").\(^ {131}\) ANDAs allow the United States Food and Drug Administration ("FDA") to speed up the timeframe in which drug manufacturers can provide to the public safe, effective, low cost alternatives to name-brand drugs.\(^ {132}\) Similarly, compulsory licensing for disease gene patents would ensure that medical consumers could access more affordable diagnostic tests and seek secondary medical opinions. Compulsory licensing would eliminate the public harm of exclusive service providers for diagnostic tests while maintaining the current patent regime.

**IV. CONCLUSION**

Patent law was created to benefit the public rather than rewarding the inventor for his or her efforts. With the recent evidence suggesting that in practice, patents do not foster scientific progress and innovation, it is time for Congress to readdress whether the current patent regime is constitutional as applied. In particular, disease gene patents may deny patients access to secondary medical opinions, which may be essential to making well-informed life-changing decisions.

The Supreme Court in *Myriad* correctly applied the statutory and judicial tests for patent eligibility but failed to address the public policy concerns that Myriad’s patents raised. In *Myriad*, both the Federal Circuit and the Supreme Court refused to address whether patients suspected of having an increased risk of developing breast cancer are entitled to a second medical opinion, but that lingering question is crucial for patients facing dire medical diagnoses.\(^ {133}\) Myriad holds the patent to the only BRCA1/2 test, which can identify an increased risk of breast and ovarian cancer. Like Lisa, women may face costly and life-changing decisions if Myriad’s test comes back positive for genetic cancer mutations. Because Myriad provides the only cancer test, patients are unable to seek a second medical opinion before accepting Myriad’s diagnosis.

The Federal Circuit and Supreme Court explicitly rejected the Petitioners’ arguments that Myriad’s gene patents limited patients’ access to care, but this issue cannot be ignored for much longer. The

---


\(^ {132}\) Id.

\(^ {133}\) Ass’n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107 (2013); Ass’n for Molecular Pathology v. U.S. Patent & Trademark Office, 689 F.3d 1303 (Fed. Cir. 2012).
Supreme Court correctly applied the law as it stands, but Congress may be forced to address whether disease gene patents violate public policy and whether they must amend present patent law.

Unlike other patents, disease gene patents enable the monopolization of testing services. Drug patents prohibit competitors from copying the patented treatment, but disease gene patents create monopolies on the testing services themselves. Monopolies of diagnostic tests inhibit physicians’ ability to practice medicine and prevent patients from attaining secondary medical opinions before undergoing costly and often life-changing treatments. Diagnostic test monopolies are fundamentally at odds with good medical practice, but the Supreme Court was correct in its application of patent law to disease gene patents. Disease gene patents can certainly constitute patent-eligible subject matter, but they ultimately do more harm to the public than good. Compulsory licensing of diagnostic gene patents is a necessary and reasonable compromise to this harm.

The Leahy-Smith America Invents Act was long overdue when it was enacted in 2011 and it only made minor changes to the present patent structure, so it is unlikely Congress will address patent law any time soon, but until they do, the courts may only continue to attempt to apply the law correctly. Courts cannot invalidate patents that satisfy the requirements of 35 U.S.C., even if the results are not beneficial to the public. If the underlying goal of patent law is to benefit the public rather than rewarding the inventor for his or her efforts, then Congress should consider whether disease gene patents benefit the public or cause unjustified harm. Ultimately, any change to the patent system has to come from Congress, not the courts. Until then, the courts may continue coming to the correct legal determinations but causing the wrong result, leaving people like Lisa out to dry.

---

THE USE OF TRADEMARKS AS METATAGS IN EUROPE: EXPANDED PROTECTIONS FROM THE EUROPEAN COURT OF JUSTICE

Emily Thornton†

I. INTRODUCTION .......................................................... 489
II. WHAT IS A METATAG? ................................................. 490
III. THE USE OF TRADEMARKS IN METATAGS: THE U.S. POSITION .......................................................... 491
   A. THE LACK OF CLEAR STATUTORY GUIDANCE .......... 491
   B. INCONSISTENT TREATMENT BY THE COURTS .......... 492
IV. THE USE OF TRADEMARKS IN METATAGS: THE EUROPEAN POSITION .......................................................... 495
   A. EUROPEAN LAW AT THE COMMUNITY LEVEL ........... 495
      1. Prohibitions Against Misleading Advertising ........ 495
      2. Trademark Protection Laws ................................ 497
   B. THE APPLICATION TO METADATA: INDIVIDUAL MEMBER STATES REACH DIFFERENT CONCLUSIONS. 498
      1. The United Kingdom ......................................... 498
      2. Germany ........................................................ 500
      3. Other Decisions from Europe ............................. 501
V. GUIDANCE FROM ABOVE: BELGIAN ELECTRONIC SORTING TECHNOLOGY NV V. BERT PEELAERS ............ 502
   A. PROCEDURAL HISTORY ......................................... 503
   B. THE EUROPEAN COURT OF JUSTICE OPINION .......... 504
VI. IMPLICATIONS FOR CONDUCTING INTERNET

† B.A. Political Science, B.S. Criminal Justice, Loyola University Chicago (2006); J.D. Candidate (2014), Wake Forest University School of Law; Staff Member, Wake Forest Journal of Business and Intellectual Property Law (2012-14). The Author would like to especially thank her daughters Chloe and Adeline for their love and inspiration as well as Tom Ferrell for his unconditional support throughout this process. Additionally, the Author would like to thank the editors and staff members of the Wake Forest Journal of Business and Intellectual Property Law for their many hours of hard work to prepare this Article for publication.
BUSINESS IN EUROPE ................................................................. 506
A. THE EFFECT OF THE PEELAERS DECISION .................. 506
B. WHAT SHOULD AMERICAN BUSINESSES DO TO
   STAY WITHIN THE LAW WHEN CREATING THEIR
   INTERNET PRESENCE IN EUROPE? ................................. 507

VII. CONCLUSION ........................................................................ 508
I. INTRODUCTION

The U.S. and Europe are each other’s most important commercial markets.¹ This is not surprising considering the substantial ties between the U.S. and EU markets. U.S.-EU merchandise trade totaled $650 billion in 2012.² At the global level, 51% of the total U.S. service sales were in Europe.³ This strong economic connection is not limited to basic trade; American businesses have made major investments in Europe. Of the $21 trillion in American corporate foreign assets, $12 trillion are in Europe.⁴ U.S. investments are not limited to private businesses; from 2000-2009, 56% of all U.S. Foreign Direct Investment was in Europe.⁵ Given the size of the European market, it is no surprise that American businesses are eager to claim their share of the pie.

The most logical way for American businesses to break into the European market is through the Internet. With the click of a button, a consumer in London can purchase an item from a business in the United States. With a good website and marketing strategy, a company can truly conduct business on a global scale. Simply creating a website and sending it to Europe, however, is not as simple as it may seem. A website owner is expected to comply with the laws of the individual countries towards which the website is directed. These laws vary by country, and what may be a legal practice in one jurisdiction may subject a business owner to severe sanctions in another jurisdiction.

One emerging but problematic aspect in the development of websites is the use of metadata.⁶ Savvy website developers insert hidden data into websites to improve their visibility in internet search rankings.⁷ Some sites insert terms that are trademarked by their competitors to try to capture some of their competitor’s market share.⁸ Depending on the circumstances of each use, this could violate both American and European trademark laws. Additionally, the European

² Id. at 7.
³ Id. at 9.
⁴ Id. at 4.
⁵ Id. at 3.
⁶ See infra Parts II.B, III.B.
⁷ See infra Part I.
⁸ See infra Part I.
Court of Justice has recently expanded protections against misleading advertising to reach metatags. This opens up a whole new maze of regulations that American businesses must navigate if they want their websites to operate legally in Europe.

Part II of this article examines metatags generally, describing what they are, how they are used, and what role trademarks play in the metatag debate. Part III begins with a discussion of the lack of statutory guidelines regarding the use of metatags in the United States, and concludes with a brief discussion of some of the inconsistent treatments that metatags have received in American courts. Part IV shifts to the position of metatags in European law. This part begins with a brief discussion of both trademark and advertising law at the community level, and then looks at the specific application of this law to metatags by individual European countries. Part V details the recent European Court of Justice decision in Belgian Electronic Sorting Technology NV v. Bert Peelaers, which will, to an extent, harmonize the legal status of metatags in advertising law. Part VI begins by explaining what the Peelaers decision means to businesses that wish to use trademarks in metatags and concludes with some suggestions as to what American businesses should do to ensure that they are in compliance with European law.

II. WHAT IS A METATAG?

At its most basic level, metadata is “information about other information.” More specifically, “metadata is structured, encoded data that describes characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities.” Metatags are metadata that is embedded into a web page’s HTML code. This code is invisible to the user but can be accessed by internet search engines. The primary types of

---

9 See infra Part IV.
12 Id. at 533 (quoting Committee on Cataloging: Description and Access Task Force on Metadata, Summary Report, ASS’N FOR LIBRARY COLLECTIONS & TECHNICAL SERVS. (June 1999), http://www.libraries.psu.edu/tas/jca/ccda/tf-meta3.html (accessed March 16, 2006)).
14 Id.
metatags are “keyword” and “description” metatags.  

Keyword metatags are, theoretically, keywords related to the contents of the website. Description metatags describe the contents of the website. 

Web developers use metatags to try to improve their rankings within internet search engines. 

One way to direct more traffic to a website is to use the tradmarked terms of a competitor within a website’s metatags. As an example, suppose that Alpha Auto Company manufactures and sells a highly popular automobile called the AlphaCar. Beta Auto Company may attempt to capitalize on the goodwill of the AlphaCar by including the term “AlphaCar” in the metatags of Beta’s website. If the metatagging is done correctly, when a user searches for “AlphaCar” on the Internet, Beta’s website will appear in the search results. Potential customers may click on the Beta site instead of the Alpha site, believing that Beta sells or is in some way affiliated with the AlphaCar. Some customers may simply return to the search results and find the real AlphaCar website, while others may continue to look at, and possibly make a purchase from, Beta. The legality of this technique can be questionable when the terms used in a metatag are protected by another entity’s trademark.

III. THE USE OF TRADEMARKS IN METATAGS: THE U.S. POSITION

A. The Lack of Clear Statutory Guidance

In the United States, there are no laws that specifically address the use of trademarks in metatags. Trademark owners have been forced to turn to antiquated laws that have not been updated to reflect the realities of the current digital age. Trademarks are currently protected under the Lanham Act, which prohibits the use of another’s trademark that “is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person . . .” Whether or not a use creates a likelihood of confusion can vary between different courts.

One common approach to determining if there is a likelihood of

---

15 Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).
16 Id.
17 Id.
18 Id.
20 See id. at 766.
confusion is the test developed by the Ninth Circuit in AMF Inc. v. Sleekcraft Boats.22 This test requires the court to consider:

(1) strength of the mark; (2) proximity of the goods; (3) similarity of the marks; (4) evidence of actual confusion; (5) marketing channels used; (6) type of goods and the degree of care likely to be exercised by the purchaser; (7) defendant’s intent in selecting the mark; and (8) likelihood of expansion of the product lines.23

These factors have been gradually refined and scaled back, particularly in the context of internet cases.24 In internet cases, the key factors to emerge from the original Sleekcraft test are the similarity of the marks, the relatedness of the goods or services, and the use of the same marketing channels.25 The test is meant to be flexible, and in the context of internet cases, other factors outside of the Sleekcraft test may be relevant.26 For a trademark holder to challenge the use of its mark in a metatag, the owner must somehow fit its claim into one of these formulations of the likelihood of confusion test.

B. Inconsistent Treatment by the Courts

Because there is no federal law that specifically addresses the use of metatags, American courts have been inconsistent in their treatment of trademarks in metatags. This is not surprising considering that the courts are forced to apply dated statutes to new technologies that were not in existence at the time of enactment, leading to resolution on an ad hoc basis.27 The success or failure of a trademark owner’s challenge to the use of its trademark in a metatag largely depends upon which courthouse the owner is able to sue in. Although the case law is not entirely predictable, a sophisticated website developer can often use a trademark in a metatag in the United States without incurring liability.

The seminal case recognizing a trademark violation for the use of a trademark in a metatag is Brookfield Communications, Inc. v. West

22 AMF Inc. v. Sleekcraft Boats, 599 F.2d 341 (9th Cir. 1979).
23 Id. at 348-49.
24 Taft, supra note 19, at 759.
25 Id.
26 Id.
Coast Entertainment Corp. from the Ninth Circuit. Brookfield Communications is a company that collects and sells information about the entertainment industry. Brookfield created a searchable database of entertainment related information that was marked under the mark “MovieBuff” in 1993. Brookfield obtained a California trademark registration for “MovieBuff” in 1994 and a federal registration in 1998. In 1998, Brookfield found out that West Coast, a large video rental chain, intended to launch a website at “moviebuff.com.” This company had used the term “Movie Buff” in various forms since 1988. This website was to include a searchable database similar to the one operated by Brookfield. Brookfield filed suit under the Lanham Act, seeking an injunction to prevent West Coast from using Brookfield’s “MovieBuff” mark in the domain name or in any metatags or other hidden codes.

Among other arguments, West Coast claimed seniority on the mark, arguing that its use of “MovieBuff” would not cause a likelihood of confusion, and thus would not violate the Lanham Act. Because the mark was used in metatags and other source codes, when a user searched for “MovieBuff,” both websites appeared in the search results. The Ninth Circuit agreed that this did not cause a likelihood of confusion because West Coast’s website is clearly labeled with its name and it is unlikely that a user would mistake this website for one owned by Brookfield. The court did, however, find a trademark violation because the use of Brookfield’s metatag would cause “initial interest confusion” because users searching for Brookfield’s database will be taken to a similar database owned by West Coast. Some users will use West Coast instead, even though they know that it is a different database. By diverting Brookfield’s customers, West Coast improperly benefited from goodwill generated by Brookfield’s

28 Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036, 1065 (9th Cir. 1999).
29 Id. at 1041.
30 Id.
31 Id. at 1042.
32 Id.
33 Id.
34 Id.
35 Id. at 1043.
36 Id.
37 Id. at 1062.
38 Id.
39 Id.
40 Id.
41 Id.
Diverting a customer’s initial interest is a form of confusion that the Lanham Act seeks to prevent. The court noted that “[u]sing another’s trademark in one’s metatags is much like posting a sign with another’s trademark in front of one’s store.” The Brookfield court remanded the case, instructing the district court to enter a preliminary injunction in favor of Brookfield.

Not all courts agree with this billboard analogy, finding it difficult to qualify this issue of initial interest confusion as a viable theory of infringement. Even if this theory is accepted, there are still other ways around an infringement suit. One way out of liability is nominative fair use. In Playboy Enterprises, Inc. v. Welles, Terry Welles used the marks “Playboy” and “Playmate” as metatags in her website. Welles was designated by Playboy magazine as its 1981 Playmate of the Year. Her website included biographical information, pictures, and information about purchasing her services as a spokesperson as well as purchasing photographs. Playboy filed suit, alleging copyright infringement.

The Ninth Circuit sided with Welles, holding that the use of Playboy’s trademarks was a permissible, nominative use. For a use to be nominative, the product or service must not be easily identifiable without the trademark, the use of the mark must be limited to what is reasonably necessary to identify the product or service, and the user must not do anything with the mark that suggests endorsement or sponsorship by the trademark holder. This test is used instead of the likelihood of confusion test because nearly all nominative uses of a trademark would be confusing. In this case, the court found that there was no reasonable way for Welles to identify herself without using the terms “Playboy” and “Playmate.” Since there is no

---

42 Id.
43 Id. at 1063.
44 Id. at 1064.
45 Id. at 1066-67.
46 See, e.g., Bihari v. Gross, 119 F. Supp. 2d 309, 320 n.15 (S.D.N.Y. 2000) (arguing that the “highway billboard metaphor is not the best analogy to a metatag on the Internet” because the harm caused by a misleading metatag is easy to correct, whereas the harm caused by a misleading billboard is not easy to correct).
47 Playboy Enters., Inc. v. Welles, 279 F.3d 796, 800 (9th Cir. 2002).
48 Id.
49 Id. at 799.
50 Id.
51 Id. at 803.
52 Id. at 801.
53 Id.
54 Id. at 804.
reasonable substitute, prohibiting the use of these marks as metatags would “have the unwanted effect of hindering the free flow of information on the Internet,” which is “certainly not a goal of trademark law.” These metatags also easily met the second and third requirements of the test. The court did, however, state that its conclusion may be different if the metatags were used extensively enough to cause Welles’s website to regularly appear above Playboy’s in internet search results. Nominative use was successfully used by Welles to get around liability under the initial interest confusion test articulated by the same circuit in *Brookfield*.

### IV. THE USE OF TRADEMARKS IN METATAGS: THE EUROPEAN POSITION

As is the case in the United States, Europe does not have a comprehensive legal regime to address the use of trademarks in metatags. The holders of trademark rights have had to attempt to claim protection through the existing laws. This section examines some of the laws used to regulate metag tag use as well as some of the court decisions rendered by individual European countries that have had to grapple with the issue.

### A. European Law at the Community Level

#### 1. Prohibitions Against Misleading Advertising

The European Council initially addressed misleading advertising in 1984. Because the initial legislation was extensively amended over the years, the misleading advertising regulations were overhauled in 2006 to ensure clarity. Regulation at the community level was enacted because advertising in Europe “reaches beyond the frontiers of individual Member States” and “has a direct effect on the smooth functioning of the internal market.” Misleading advertising was

---

55 The district court suggested that Welles identify herself as “the nude model selected by Mr. Hefner’s organization.” *Id.*
56 *Id.*
57 *Id.*
58 *Id.*
61 *Id.* at pmbl. 2.
targeted because it can distort competition within the internal market. Standardization in advertising laws was established because “the differences between the laws of the Member States” was hindering multinational advertising campaigns, which in turn was impacting “the free circulation of goods” and services.

Under Directive 2006/114, advertising is misleading if it:

in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behavior or which, for those reasons, injures or is likely to injure a competitor.

Member States are directed to have “adequate and effective means” to combat misleading advertising. This requires legal provisions against misleading advertising as well as avenues for aggrieved parties to pursue complaints through a judicial or administrative system. The specific means by which this is accomplished is left to the discretion of each member state.

This directive also addresses the use of comparative advertising, which is defined as “any advertising which explicitly or by implication identifies a competitor or goods or services offered by a competitor.” This directive allows comparative advertising when it is not misleading and compares goods or services that are intended for the same purpose or that meet the same needs. However, this directive is highly protective of trademark rights. It does not allow comparative advertising that denigrates, takes unfair advantage of, creates confusion with, or imitates a protected trademark. This directive creates a floor; Member States are allowed to implement more extensive regulations.

---

62 Id. at pmbl. 3.
63 Id. at pmbl. 5.
64 Id. at art. 2(b).
65 Id. at art. 5(1).
66 Id. at art. 5.
67 Id.
68 Id. at art. 2(c).
69 Id. at art. 4(a)(b).
70 See id. at art. 1, art. 8(1).
71 Id. at art.4(d), 4(f), 4(g), 4(h).
72 Id. at art. 8(1).
2. Trademark Protection Laws

Trademark law in Europe is, at times, complex, because a registrant may have to navigate both national trademark systems as well as community level requirements. The Council first addressed the harmonization of national trademark laws in 1989 because there were enough disparities between national laws to “impede the free movement of goods and freedom to provide services” and to “distort competition within the common market.”73 This directive created a basic framework for national trademark systems, setting basic standards such as what may be trademarked, grounds for refusal of a trademark, and the basic rights conferred by a trademark.74 Each member country was required to implement these basic requirements by the end of 1991.75 While this directive harmonized many more fundamental aspects of national trademark laws, it did not eliminate national trademarks. The substantive law interpretations of it still vary across individual countries, much like the law in the United States can often vary between states or federal circuits.

In an attempt to further integrate the market and simplify regulation, a community level trademark system was developed in 1993.76 This allows a registrant to register a trademark at the community level, which gives it protection in all Member States.77 Instead of filing individual applications in every country, one application is filed with the newly created Office for Harmonization in the Internal Market.78 Registration for the community trademark opened in 2006.79 A community trademark application can be opposed if the mark requested is identical to an earlier trademark, or if it would create a likelihood of confusion with an earlier trademark.80 This means that a community level application is precluded if the mark is already recognized by the national laws of any member country and its owner objects to the community application.81

Theoretically, national trademarks could become unnecessary as registrants shift from individual national marks to the community

---

74 See id. at art. 1-15.
75 Id. at art. 16(1).
77 Id.
78 Id.
79 Id.
80 Id. at art. 8.
81 Id.
mark. Despite the obvious benefits of community wide protection, the national registries are still holding strong. Of the approximately 540,000 annual trademark applications in Europe, only 10% are filed at the community level. Smaller businesses and geographically isolated businesses tend to prefer their local systems over the community system. This means that anyone registering a trademark in Europe, or anyone that may be infringing upon a European trademark, must continue to be aware of both national and community level regulations.

Significant change is on the horizon for both national and community trademark law. In June 2013, changes to both the community system and the national systems were proposed because the current system is outdated, harmonization has been limited, and there are inconsistencies between the Directive on national trademarks and the Directive on the community mark. The reforms will make the registration systems more accessible and will lower the cost and complexity of the application process while increasing the legal predictability of the system. The system-wide office practices will be converged with the goal of developing common databases to facilitate cooperation between the national offices and the community office. The new reforms will also incorporate a substantial amount of case law from the European Court of Justice directly into the legal provisions governing both systems. The changes are expected to be adopted in the spring of 2014 with a two year timeframe for implementation. This adds an additional layer of complexity for those that are planning to expand into Europe, as the rules are set to change at both the national and community level.

B. The Application to Metadata: Individual Member States Reach Different Conclusions

1. The United Kingdom

Like the United States, the United Kingdom does not have any comprehensive legislation addressing the use of metatags. The leading
UK case to challenge the use of a trademark in a metatag was made under the UK Trademarks Act of 1994, which implemented the Community level Trade Marks Directive 89/104. In this case, the Court of Appeal reversed a trial court decision granting relief to the trademark owner.90

The plaintiff, Alec Reed, started an employment agency in 1960, which matched potential employees to businesses that were hiring.91 The company registered the trademark “Reed” in 1986 when trademark protection initially became available.92 The company continued to expand, and by 1996 was operating a website under the URL “www.reed.co.uk.”93 The defendant was Reed Business Information Ltd., a publishing company that published around fifty magazines and journals.94 These publications included extensive job advertising sections.95 In 1999, Reed Business Information created a dedicated employment advertising website under the URL “www.totaljobs.com.”96 The totaljobs website included various forms of “Reed Business Information” as hidden metatags.97

The trial court found that this use of the trademark “Reed” constituted infringement because the defendant’s use “passed off their business and services as and for those of the Claimants herein by the use in connection therewith of the word ‘Reed.’”98 By using the trademark “Reed,” the “ultimate purpose . . . is to use the sign to suggest a connection which does not exist.”99 On appeal, the appellate court reversed, noting that “[o]bviously anyone looking for Reed Employment would find them rather than totaljobs” and that “[n]o-one is likely to be misled – there is no misrepresentation.”100 The court found that “causing a site to appear in a search result, without more, does not suggest any connection with anyone else.”101 The ability to challenge the use of trademarks in metatags in general was questioned, because “[u]ses read only by computers may not count – they never

---

90 Reed Executive Plc v. Reed Business Information Ltd., [2004] EWCA (Civ) 159, [14] (Eng.).
91 Id. at [150].
92 Id. at [4].
93 Id. at [5].
94 Id. at [7].
95 Id. at [2]-[3].
96 Id. at [3].
97 Id. at [8].
98 Id. at [147].
99 Id. at [16].
100 Id. at [148].
101 Id. at [148].
convey a message to anyone.” Although hiding a competitor’s trademark in a metatag may be unfair to some, the court noted that others find this to be “good competition provided that no-one is misled.” This decision appears to take a fairly pragmatic approach to the use of trademarks in metatags, upholding their use unless there is some kind of obvious unfairness to the trademark holder.

2. Germany

In Germany, the use of trademarks in metatags was previously controversial because lower courts and academics disagreed on whether or not the use of a trademark in a metatag constituted use under applicable law. In 2006, the German Federal Supreme Court settled the issue, holding that a metatag constitutes use of a designation in the course of trade, which is a trademark use. The plaintiff in this case operated a website under the company name “Impuls Medienmarketing GmbH,” that provided free consulting services, including comparisons between thirty-five private health insurance plans. The defendants were former freelance employees and partners of the plaintiff who operated a similar website offering the same services as Impuls. The defendants used the term “Impuls” as a metatag, resulting in the defendant’s website appearing in search results when a user searched for the term “Impuls.” The plaintiffs filed suit, alleging trademark infringement, and sought an injunction to end the use.

The Supreme Court held that it is not relevant that the metatag is not visible because it still influences search results and directs users to the metatagged website. A likelihood of confusion can exist because a user may be misled by the metatag to believe that the tagged site belongs to or is associated with the owner of the protected trademark. The Court also held that the use of a metatag can be

102 Id. at [149].
103 Id.
104 See Jonas Rechtsanwaltsgesellschaft, Germany, WORLD TRADEMARK REVIEW Apr./May, 2009, at 69.
105 See Bundesgerichtshof [BGH] [Federal Court of Justice] May 18, 2006, I ZR 183/03, 2006 (Ger.).
106 Id. at (1).
107 Id. at (2).
108 Id.
109 Id.
110 Id.
111 Id. at (5).
112 Id.
actionable under the Act against Unfair Competition as an act of unfair obstruction.\footnote{113}

This German decision is much more protective of trademark holders than the Reed decision from England. The mere fact that the metatag has caused the defendant’s website to appear in the search results for the trademarked term is enough for a likelihood of confusion in Germany, whereas it was not sufficient in England.

3. Other Decisions from Europe

As demonstrated by the case law in England and Germany, different countries come to different conclusions about the use of trademarks in metatags. This makes it difficult to predict whether or not the use of a trademark in a metatag is acceptable across Europe. Additionally, in many countries this is a new area of law that has not been finally settled. This section provides a brief description of some of the metatag case decisions in other European countries.

Denmark provides some protection for trademark holders when it comes to metatags. In Coffilter Int’l ved Jørgen Byrial Petersen v. Melitta SystemService Aromateknik, the Denmark court determined that the use of a trademark in a metatag alone, when the mark is not part of a comparative statement, “constitutes infringement.”\footnote{114} The court further held that if the trademark is used within a comparative statement, it is acceptable.\footnote{115} Finally, the court held that even if the trademark is used in a metatag for a permitted purpose such as for comparative purposes, it still must be used “in accordance with honest practices.”\footnote{116}

Spain recently issued its first opinion regarding metatags in Maherlo Ibérica S.L. v. Calzados Fernando García S.L.\footnote{117} This dispute was between two companies that sell elevated shoes.\footnote{118} One company used the trademarked term “MasAltos” (higher) in the metatags and Google Adwords of its website.\footnote{119} The court found a

\footnote{113} Id.
\footnote{115} Id.
\footnote{116} Id.
\footnote{117} Hogan Lovells, Ana Castedo & Eugenio Vasquéz, First Decision by Spanish Court on the Use of Trademarks as Keywords in Google’s Adwords and Metatags, LEXOLOGY (July 20, 2012), http://www.lexology.com/library/detail.aspx?g=a1e6e1a7-2a70-4098-9647-aa7de535f316.
\footnote{118} Id.
\footnote{119} Id.
trademark violation because this use diminished the distinctiveness of the trademark holder’s mark.\textsuperscript{120} This occurs because the Internet user is not able to determine whether the marketed products belonged to the trademark holder, or to a third party.\textsuperscript{121}

In Denmark, Belgium, and Austria, plaintiffs have been able to successfully bring infringement claims for the use of a trademark in a metatag.\textsuperscript{122} In France, there is not a uniform rule, and the issue seems to be decided on a case-by-case basis.\textsuperscript{123} In some cases, such as S.A.R.L. CNRRH v. S.A.R.L. 2L Multimedia, the courts have dismissed infringement claims based on metatags.\textsuperscript{124} In other cases, such as Webangelis v. Laurent I, the courts have found infringement when a competitor’s trademark was used in a hidden metatag.\textsuperscript{125} Like American law, French law is not yet entirely settled.

\section*{V. Guidance from Above: Belgian Electronic Sorting Technology NV v. Bert Peelaers}

Thus far, challenges by trademark holders to the use of their marks in metatags have proceeded under the trademark laws of the respective countries.\textsuperscript{126} Since there is no set law governing metatags, some plaintiffs have gotten creative and pressed for protection under advertising laws.\textsuperscript{127} In Belgian Electronic Sorting Technology NV v. Bert Peelaers, the European Court of Justice expanded the definition of “advertising” in Directives 84/450/EEC and 2006/114/EC to include the use of metatags.\textsuperscript{128}

\begin{thebibliography}{99}
\bibitem{footnote120} Id.
\bibitem{footnote121} Id.
\bibitem{footnote122} Online Advertising and Use of Others’ Marks, INT’L TRADEMARK ASS’N, http://www.inta.org/TrademarkBasics/FactSheets/Pages/OnlineAdvertisingandUseofOthersMarksFactSheet.aspx (last visited Nov. 18, 2013).
\bibitem{footnote123} Id.
\bibitem{footnote124} Id.
\bibitem{footnote125} Id.
\bibitem{footnote126} See supra Part III.B.
\bibitem{footnote128} Id. ¶ 39. This case also addressed two separate issues: the registration of a trademark as a domain name and the use of that trademarked domain. The court held that the mere registration of a domain is not use within the meaning of the directives. Id. ¶ 43. The court did, however, hold that using a domain name that consists of a trademarked term is use and therefore falls within the protections of the directives. Id.
\end{thebibliography}
A. Procedural History

This case involved a trademark dispute between BEST and Visys, two companies that produced, manufactured, and distributed sorting machines.\textsuperscript{129} BEST was established in 1996 and produced sorting machines named “Helius,” “Genius,” “LS9000,” and “Argus.”\textsuperscript{130} Visys was established in 2004 when Bert Peelaers, a BEST employee, left BEST to set up his own company that directly competed with BEST.\textsuperscript{131} In 2007, Peelaers registered the domain www.bestlasersorter.com on behalf of Visys, which hosted the identical content as his other domain names (www.visys.be and www.visysglobal.be).\textsuperscript{132} Visys used the metatags Helius sorter, LS9000, Genius sorter, BEST+Helius, BEST+Genius, and BEST nv on this website.\textsuperscript{133} In 2008, BEST applied for the Benelux figurative trademark BEST.\textsuperscript{134}

After applying for the trademark, BEST filed suit, alleging that the registration and use of the domain name www.bestlasersorter.com and the use of the metatags both infringed on BEST’s trademark rights and violated the laws on misleading and comparative advertising.\textsuperscript{135} Visys responded with a counterclaim seeking to annul the Benelux mark BEST.\textsuperscript{136} At the trial court level, the Antwerp Commercial Court in Belgium dismissed all of BEST’s claims, except the claim alleging Peelaer’s use of metatags violated laws regulating comparative and misleading advertising.\textsuperscript{137} On appeal before the Antwerp Court of Appeal, however, every one of BEST’s claims were dismissed.\textsuperscript{138} BEST then lodged an appeal with the Court of Cassation, which dismissed the trademark infringement claims.\textsuperscript{139}

Before deciding the claims under the comparative and misleading advertising laws, the Court of Cassation stayed the case and asked the European Court of Justice for a preliminary ruling to interpret the term “advertising,” as used in Directives 84/450 and 2006/114.\textsuperscript{140} The question referred was: “[i]s the term ‘advertising’ in Article 2 of
[Directive 84/450] and in Article 2 of [Directive 2006/114] to be interpreted as encompassing, on the one hand, the registration and use of a domain name and, on the other, the use of metatags in a website’s metadata.” The Belgian and Italian governments intervened to argue that the use of metatags was encompassed by advertising under these directives. The Polish government and the European Council argued that metatags did not fall within the definition of advertising.

B. The European Court of Justice Opinion

The European Court of Justice began its analysis by determining what “advertising” means under Directives 84/450 and 2006/114. Both Directives define advertising as “a representation in any form made in connection with a trade, business, craft, or profession in order to promote the supply of goods or services.” Prior case law has construed this definition liberally, holding that it is not limited to traditional forms of advertising. The purpose of both Directives was to provide protection from the unfair consequences of misleading advertising and to set the guidelines for when comparative advertising is allowed. These Directives sought to balance everyone’s interests by allowing comparative advertising that objectively highlights the benefits of comparable products while prohibiting advertising that adversely affects competition and consumer choice.

The Court concluded that the Directives were intended by the European Union legislature to establish a complete framework for all forms of advertising. Therefore, any “steps taken by a trader to promote the sale of his products or services that are capable of influencing the economic behavior of consumers and, therefore, of affecting the competitors of that trader” are subject to these directives. With this broad conception of advertising in mind, the Court turned to the specific use of metatags.

The Court recognized that metatags are used by search engines when they reference websites and constitute one of the factors that allow a site to be ranked according to relevance when an Internet user

141 Id.
142 Id. ¶ 33.
143 Id.
144 Id. ¶ 34.
145 Id.
146 Id. ¶ 35.
147 Id. ¶ 36.
148 Id. ¶ 37.
149 Id. ¶ 38.
150 Id. ¶ 39.
enters a search term. When the name of a competitor is used in a metatag and an Internet user searches for the goods of that competitor, the result displayed will be changed to include the user of the metatag in the search results. In some cases, the metatag user’s website will be displayed directly next to the competitor’s website. Indeed, when a user searches for “Best Laser Sorter” in www.google.be, the BEST website is the first result followed directly by the Visys website.

In most cases, the Court found that when an Internet user searches for a company’s name or product, the user is looking for information about that specific company or product. If a competitor’s website is displayed among the first search results, the user may perceive the competitor’s website as offering the searched for goods or services. Because the use of a trade name in the programming of a website suggests that the searched term is related to the site, this use was held to be a representation under Directives 84/450 and 2006/114.

The Court went on to conclude that it does not matter that a metatag is invisible to the Internet user. Under the very broad definition of advertising discussed above, advertising encompasses “any form of representation,” including “indirect forms of representation” that are “capable of influencing the economic behavior of consumers and, therefore, of affecting the competitor whose name or goods are referred to by the metatags.” The Court determined that there was “no doubt” that this use of metatags was a “promotion strategy” that “aims to encourage the Internet user to visit the site of the metatag user to take an interest in its goods or services.” Therefore, the use of metatags in this situation is encompassed by the term “advertising” under Directives 84/450 and 2006/114.

---

151 Id. ¶ 53.
152 Id. ¶ 54.
153 Id.
154 Id. ¶ 55.
155 Id. ¶ 56.
156 Id.
157 Id. ¶ 57.
158 Id. ¶ 58.
159 Id.
160 Id. ¶ 59.
161 Id. ¶ 60.
VI. IMPLICATIONS FOR CONDUCTING INTERNET BUSINESS IN EUROPE

A. The Effect of the Peelaers Decision

This case was referred to the European Court of Justice by the Belgian Hof van Cassatie (Court of Cassation) for a preliminary ruling on the correct interpretation of “advertising” under the false advertising directives.\(^\text{162}\) A preliminary ruling has the force of res judicata.\(^\text{163}\) This means that the holding is binding on both the Belgian court that referred the case, as well as the national courts of all of the Member States.\(^\text{164}\) After this case, the use of a metatag will, therefore, be considered to be advertising in all Member States. This decision opens the door to suits under the misleading advertising laws of all Member States. The plaintiffs won at the community level in this case, but they only won the ability to open up the door. The European Court of Justice did not decide whether or not Peelaer’s use of the trademarks was in fact misleading.\(^\text{165}\) The case was referred back to the Belgian court system for a determination in the first instance whether or not the metatags were misleading.\(^\text{166}\) The plaintiffs now have a viable cause of action but may still lose the case on the merits.

The true impact of this decision will vary by country, as this decision may be more or less liberal than each country’s current laws. If a Member State has previously declined to extend advertising to include metatags, or if the issue has never arisen, then this case creates a pretty significant change in the law. While the Belgian and Italian governments intervened to argue that metatags were advertising, the European Council and Poland disagreed.\(^\text{167}\) If a country is more liberal in its advertising laws like Belgium and Italy, then this decision may not be a major change. In either situation, it does bring with it some degree of certainty: metatags are now considered to be a form of advertising, and under Directives 84/450 and 2006/114, their use cannot be misleading.\(^\text{168}\)

\(^\text{162}\) Id. ¶ 26.
\(^\text{164}\) Id.
\(^\text{165}\) Peelaers, Case C-657/11 ¶ 61.
\(^\text{166}\) Id.
\(^\text{167}\) Id. ¶ 33.
\(^\text{168}\) Id. ¶ 61.
B. What Should American Businesses Do to Stay within the Law When Creating Their Internet Presence in Europe?

Europe now has a very broad definition of advertising. Any business that is considering operating in Europe must understand that metatags, while visually hidden, are still considered to be advertising. The use of a metatag now subjects the site owner to liability under the advertising laws of the European Union, as well as the advertising laws of each individual country.

Before using a competitor’s mark in a metatag, a business should thoroughly research both the trademark and advertising laws of any country in which the website will be operating. If unsure of the legal consequences, a company may be well advised to avoid the questionable use. Violations subject the business to litigation in multiple national court systems, as well as the Community justice system. This is incredibly time consuming, expensive, and complicated. Any competitive advantage gained may not be worth the resulting costs and hassle of an international, multi-national legal battle.

Additionally, the legality of a specific metatag use still may not be consistent across Europe. Although all metatag uses now must not be misleading, it is likely that different countries will have different ideas of what misleading means. Thus far, England appears to be very liberal. Under Reed, the court found the questioned metatag use to be “good competition” and stated that it was obvious that the two websites were owned by different companies. If the BEST case were tried before a British court, it is likely that BEST’s claim would fail because it would be apparent that Visys was a separate company from BEST and that it was not actually selling BEST products. In Germany, a likelihood of confusion was enough for the Federal Supreme Court to find a violation. BEST would likely prevail in German courts because a user could be confused if the Visys website appeared when searching for BEST. If a business intends to isolate itself within one geographic area, it may be possible to predict, with

---

169 See supra Part V.A.
170 See id.
171 For example, the BEST case has gone through three levels of the Belgian court system, an interlocutory appeal to the European Court of Justice, and now must work its way back through the Belgian court system again. The case has been active for five years and is still ongoing.
172 See supra Part III.B.1.
173 Reed Executive Plc v. Reed Business Information Ltd., [2004] EWCA (Civ) 159, [149] (Eng.).
174 See supra Part III.B.2.
reasonable certainty, which way one or two national court systems will treat the issue. If, however, a business intends to have a broad European presence, it is unlikely that it can fashion a website with trademarked metadata that does not offend the trademark and advertising laws of at least one country.

If a business is insistent upon using metadata, some uses are more likely to be acceptable than others. Using a competitor’s mark solely to redirect Internet traffic from the competitor’s site is likely misleading. This inherently makes sense; unfairly capitalizing on a company’s goodwill to bait and switch a potential customer should be avoided. Even the Reed court recognized that it would be a violation of the law if the customer was actually misled.175 Additionally, purely comparative uses are likely acceptable everywhere. The real issue is the gray area in between where the metadata user is not really comparing products, but has not gone as far as to outright mislead customers.

Before taking a risk by using metatags, a business should ask itself what it would truly gain in the process. Some search engines claim that they no longer consider metatags when compiling their search results. Google stated that the main Google search page “disregards keyword metatags completely” because “the keyword metatag was so often abused.”176 Despite the questionable utility of using metatags, web developers have used and will likely continue to use them. As demonstrated by the American and European cases discussed here, companies use and fight about the use of metatags regularly.177 Additionally, the ineffectiveness of a metatag does not make it legal. Any company seeking to use a competitor’s trademark should think twice before taking an enormous legal risk for a likely small, or nonexistent, reward.

VII. CONCLUSION

Any time technology advances, it brings with it new and innovative opportunities. In this day and age, the Internet has become incredibly important to anyone operating a commercial business. Markets that were previously unreachable are now easily accessible with the touch of a button. Businesses are eager to capitalize on their share of the Internet market, utilizing new and developing means to

175 Reed [2004] EWCA (Civ) 159, at [149].
177 See, e.g., supra Parts II.B, III.B.
get ahead. While it is tempting to jump right into newly emerging technologies, businesses should take a step back to fully examine the legal ramifications of using new technology. This is particularly important when venturing into foreign legal jurisdictions.

The use of metatags is one such new technology that should be used with caution, particularly when it comes to the use of another’s trademark. There are no specific, on point laws that govern the use of metatags, and the case law on the issue is unsettled in the United States. It is also unsettled in Europe, both between different countries and, at times, within a single country. Although the European Court of Justice has now mandated that metatag use must conform to the laws on false and misleading advertising, there is still a lot of room for different interpretations of what is or is not misleading. The safest option for any business with an Internet presence in Europe is to avoid using someone else’s trademark in a metatag unless it is used for purely comparative reasons. The risk of being hauled into a foreign court is very real and is likely not worth the resulting costs.