Blockchain: The Future of All Data

MARIO ISKANDER*

INTRODUCTION

This comment is organized in four parts. Part I describes how Privacy Policies and Terms of Conditions are difficult to understand and inherently incomplete. It provides an overview of the legal landscape for these types of contracts, identifying some of the legal hurdles companies have to maneuver to be able to use these contracts online. Part II gives a further overview and describes the Ricardian contract and how blockchain will improve the lives of consumers by laying an initial background then illustrating the technical and useful sides of these technologies. Part III reviews the rules existing in federal law, describing what they do and how they interact with each other, with the addition of some cases that have arisen regarding medical devices ("mdevices"). Part IV describes some of the gaps that federal regulation has created and how some States have filled in these gray areas of law.

PART I

Online Privacy Policy and Terms and Conditions agreements are mandatory because companies collecting health data can use that data to identify an individual.[1] Even though there isn't a single federal law that *requires* all companies in the United States to have online agreements, many federal and state laws *suggest* that these companies should under specific circumstances.[2] Some of these federal and state laws that have provisions on data privacy include the Americans With Disability Act, the Cable Communications Policy Act of 1984, the Children's Internet Protection Act of 2001 (updated in 2013), the Computer Fraud and Abuse Act of 1986, and the Computer Security Act of 1997. The Federal Trade Commission is the federal agency that regulates data protection of all consumers in the USA.[3] Most online legal agreements are presented to users through either a Clickwrap or Browsewrap agreement.[4] A Browsewrap agreement is

---

*Mario Ashraf Iskander Henein is a 2018 J.D. Candidate at the University of San Francisco School of Law. He earned his B.A. from California State University Fullerton. Mario would like to thank Mike De Smidt, Daniel Gaitan, and all of the staff from the ITPLJ that helped this comment arrive in its final form. Mario would also like to thank Dean Susan A. Freiwald, Prof. David Franklyn, Joshua de Larios-Heiman, and his family for their constant support and inspiration.

1. *Privacy Policies Are Mandatory By Law*, TERMSFEED (Sep. 18, 2017) https://termsfeed.com/blog/privacy-policy-mandatory-law/.

2. *Id*.

3. *Id*.

4. Alison S. Brehm & Cathy D. Lee, From the Chair: "Click Here to Accept the Terms of Service," COMM. LAWYER, VOL. 31, NO. 1, available at: http://www.americanbar.org/publications/communications_lawyer/2015/january/…

omnipresent throughout a website.[5] It's usually a link at the bottom of the web page that sends the user to the Privacy Policy or a Terms and Conditions page. Instead of requiring the user to manually agree by clicking on an "I agree" button,[6] the user implicitly agrees by using the website. If a website uses a Browsewrap agreement, it is more likely that a user has had the opportunity to see and read the Terms and Conditions agreement, and more likely a court will enforce the Terms and Conditions agreement against that user.[7]

Clickwrap agreements differ from Browsewrap agreements because Clickwrap agreements require users to check or toggle an "I agree" checkbox in order to continue to the rest of the website.[8] Privacy Policies and Terms and Conditions are given increased notice in front of a user to increase the likelihood that the user read the agreements, understood, and agreed to the terms before using the website. Thus, Clickwrap agreements allow the user to physically consent to the website's terms.[9]

Unfortunately, there are no bright line rules when it comes to the enforceability of Browsewrap or Clickwrap agreements.[10] However, there are a variety of ways website owners can increase the likelihood that these agreements will be enforced, such as a check-box that users must click adjacent to an affirmation similar to, "[b]y clicking on the box, you are indicating that you have read and agree to the Terms of Use." Some other suggestions include: A webpage that is designed so that if the user does not check the box manifesting assent to the terms, the user cannot proceed in the transaction; Making the terms of use available either in a nearby scrolling text box or a nearby hyperlink;

Any hyperlink of the terms that is obvious, such as "Terms of Use" is underlined and has decent size lettering and visible coloring;

Any hyperlink of the terms that has a central or obvious location on the webpage, e.g., the hyperlink is located directly below the "I Agree" button and not relegated to the bottom of the webpage, which would require the user to scroll down to a different portion of the webpage;

Any hyperlink of the terms that immediately displays the terms instead of requiring the user to click on a series of hyperlinks to view the terms;

Terms of use that are evident in every webpage of the website rather than being visible on only one webpage, in addition to requiring users to attest that they have read the terms.

Terms that are in readable font (and at least 12 point); and

Agreements that contain all requisite elements of an enforceable contract (e.g., consideration, sufficiently definite material terms, etc.)

---

5. *Id*.
6. *Id*.
7. *Id*.
8. *Id*.
9. *Id*.
10. *Id*.

In addition to these best practices and general principles the courts have adapted some general tests for online agreements.[11] Generally, as long as there is reasonable notice of and manifested assent to the agreement, the online agreements will not be void.[12] Below is the jurisprudence that has developed over the past several years regarding the concerns surrounding enforceability.

In *DeJohn v. The .TV Corporation*,[13] the court held that a Clickwrap agreement was valid because the plaintiff bound himself by clicking an 'I Agree' button, which indicated that he read, understood, and assented to the terms of the parties' contract.[14] The contract's terms were available for review online by clicking on a link which appeared on the Register.com website just above the 'I Agree' button.[15]

In *Forrest v. Verizon*,[16] the plaintiff claimed that Verizon had not provided it with notice of a forum selection clause.[17] The plaintiff had assented to a Clickwrap agreement that was within a scroll box and above the Clickwrap agreement were the words: "PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY."[18] The user was required to click to show that they agreed to Verizon's thirteen-page Terms of Service Agreement before they could continue with the transaction.[19] The court found that although the Terms of Service were difficult to read, the customer was provided with ample notice and consented to the terms.[20]

In *Motise v. America Online*,[21] the court enforced the forum selection clause of the service agreement against the plaintiff even though he did not accept the terms of service himself.[22] The court concluded that because his stepfather accepted terms of service, the plaintiff was bound to the terms as a sub-licensee of privileges conditionally granted to the stepfather.[23]

In *Specht v. Netscape*,[24] the appellate court reviewed a Browsewrap agreement on the Netscape website.[25] The court found that Internet users could not manifest assent and did not assent to the license agreement's arbitration clause by simply downloading free software from a website. In *Specht,* the user was presented with a download link for software and could only review the "Terms of Service" for that download by scrolling to the

11. *Id.*
12. *Id*.
13. DeJohn v. The .TV Corp., Int'l, 245 F.Supp. 2d 913 (N.D. Ill. 2003).
14. *Id*. at 918.
15. *Id*. at 919.
16. Forrest v. Verizon Commc'n, Inc., 805 A.2d 1007 (D.C. 2002).
17. *Id*. at 1010.
18. *Id*.
19. *Id*.
20. *Id*.
21. Motise v. America Online, 346 F.Supp. 2d 563 (2004).
22. *Id*. at 566.
23. *Id*.
24. Specht v. Netscape, 306 F.3d 17 (2d Cir. 2002).
25. *Id*.

next page.[26] The court stated that without the formation of mutual assent, a contract does not exist.[27] It held that since the plaintiff was not made aware of the terms before using the software, the agreement was unfair and therefore void.[28]

In *Hubbert v. Dell*,[29] customers purchasing from Dell's website were shown five Web pages of forms the buyers had to fill out to purchase.[30] On the top of the pages, there was a blue hyperlink that took a purchaser to the "Terms and Conditions of Sale."[31] The last three forms stated that all sales were subject to the terms and conditions of sale and included an arbitration clause. The court found that the Web pages' blue hyperlinks to "Terms and Conditions of Sale" of computers incorporated the conditions, including the arbitration clause, into the sales contract, and the clause was not procedurally nor substantively unconscionable.[32] The court found that the user had the ability to find and read the "Terms and Conditions of Sale" readily and did not obscure it.[33]

In *Cairo v. CrossMedia Services*,[34] the plaintiff used the Cross Media Services website several times.[35] When the plaintiff sued for declaratory judgment in a different venue than indicated in the Terms of Use, the court found that plaintiff was bound by the forum selection clause contained in Terms of Use posted on defendant's websites.[36] The court found that Cairo's repeated use of the defendants website services formed the basis that the plaintiff had knowledge of the Terms of Service agreement by virtue of using the website.[37]

JDate moved to have the case transferred to California as it was a clause in the agreement which was displayed on JDates website.[38] Zaltz had noted that she didn't remember agreeing to a forum selection clause.[39] The court found that JDate presented its users "on the same screen as the button a prospective user must click in order to move forward in the registration process."[40] The "reference to its Terms and Conditions of Service appear[s] above the button."[41] In addition, prospective members had to check a box

26. *Id*. at 20.
27. *Id*. at 29, 30.
28. *Id*.
29. Hubbert v. Dell, 359 Ill. App. 3d 976 (5th Dist. 2005).
30. *Id*.
31. *Id*.
32. *Id*. at 983.
33. *Id*. at 984.
34. Cairo v. CrossMedia Services, No. C 04-04825 JW, 2005 U.S. Dist. LEXIS 8450, at *2 (N.D. Cal. Apr. 1, 2005).
35. *Id*. at *13.
36. *Id*. at *14.
37. *Id*.
38. Zaltz v. JDate, 952 F. Supp. 2d 439 (F.D.N.Y. 2013).
39. *Id*. at 451.
40. *Id*. at 453.
41. *Id*. at 454.

stating "I confirm that I have read and agreed to the Terms and Conditions of Service," where the terms were hyperlinked.[42] Thus, the court noted that Ms. Zaltz assented to the member agreement twice.[43]

PART II

In order to understand the legal significance the Ricardian contract has on blockchains, and how it can be a solution to the health sector and the legal industry, one must first have a conceptual understanding of Smart contract, parameters, prose, code, and how these are evolving in current platforms such as Bitcoin.

SMART CONTRACT

Nick Szabo coined the phrase "smart contracts," and explained it best as follows:

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.[44]

PARAMETERS, PROSE, AND CODIFYING THE LAW

"Parameters are aspects that are specific to a particular contract, such as prices, dates and quantities."[45] A deal point is a fluid notion since any aspect of a contract can become a critical negotiation issue in a particular transaction.[46] The Ricardian contract includes both prose and parameters.[47] Parameters provide the link from prose to code. A parameter might be named in one document, given a value in a second document, and used in a third document. William Mitchell is credited with showing how [computer] code is law.[48] In real space, we recognize how laws regulate – through constitutions, statutes, and other legal codes.[49] In cyberspace, we must understand how a different "code" regulates – how the software and hardware that make cyberspace what it is also regulate cyberspace as it is.[50]

---

42. *Id*.

43. *Id*.

44. Nick Szabo, SMART CONTRACTS (1994), *available at* http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

45. Helen Happio & James Gardiner Hazard, *Wise Contracts: Smart Contracts that Work for People and Machines*, JUSLETTER IT (February 23, 2017) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2925871).

46. *Id*.

47. *Id*.

48. Lawerence Lessig, Code Version 2.0, 5, (2006).

49. *Id*.

50. *Id*.

BITCOIN

Bitcoin is a cryptocurrency that is recorded on blockchain public ledger without any centralized authority.[51] The transactions are placed in an escrow, which is controlled by the payer, creating a basic smart contract. Bitcoin has always been a cryptocurrency and even the different uses of Bitcoin have been generally focused on specialized applications and cryptocurrencies, with most of the blockchain projects being platforms for financial technology applications like Symbiont.io, R3, and Chain.com.[52]

THE FURTHER EVOLUTION OF BITCOIN?

Ethereum was promoted as an open source platform allowing users to create any project that deals with "smart contracts" transactions on its ledger.[53] The Ethereum platform features a general purpose programming language for constructing "smart contracts."[54] In fact, the original Ethereum white paper is entitled, A Next-Generation Smart Contract and Decentralized Application Platform.[55] Whether or not it will replace Bitcoin as the leading cryptocurrency is not clear, though, it appears to have a growing recognition in the legal community that has created interest in smart contracts once again.

IS RICARDIAN CONTRACT BLOCKCHAIN A SOLUTION?

Ricardian contract can store materials and handle transactions such as payments, agreements, permits, organizational documents, intellectual property, and medical histories.[56] Given that a blockchain-based smart contract is always available to users on the chain, it is a reliable source of information that can also make payments, do legal formalities, create and file reports, manage access to digital works, execute code, and arrange logistics.[57] It can also serve as a system of identification for transacting.[58] Smart contracts come with many of advantages for lawyers, the public consumer and health care providers.

ADVANTAGES FOR LAWYERS:

- All records relating to payments in a single system of management.

---

51. *See generally*, https://bitcoin.org/en/how-it-works.

52. Brent Miller, *Smart Contracts and the Role of Lawyers (Part 1) – About Smart Contracts*, BIGLAW KM, Oct. 20, 2016, http://biglawkm.com/2016/10/20/smart-contracts-and-the-role-of-lawyers-part-1-about-smart-contracts/.

53. Vitalik Buterin, *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform*, BITCOIN MAGAZINE, Jan. 23, 2014, https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/.

54. *Id*.

55. *Id*.

56. Happio & Hazard, *supra* note 45.

57. *Id*.

58. *Id*.

- Full portability of accounts.
- Integrated functionality of websites and software for management, reporting, etc.
- Codified legal
- Better management of "signature" for better informed medical consents. Basically, getting rid of the need for Clickwrap and Browsewrap. Conditions of signature could be automated or subject to second signature to avoid fraud and errors adding to efficiency and reliability.
- Reliance on a regulated organization, with local offices, employees, etc., community anchoring as the primary supplier.
- Reduce the number of persons who have copies of personal data.
- A unified approach to security.
- A semantic, graph-based, peer-to-peer system for identifying suppliers/vendors and third party associates, many of who can be closer, smaller, and more personal.

Given these features, Clickwrap and Browsewrap would no longer be necessary. Conditions of signature could be automated or subject to a second signature to avoid fraud and errors, while adding efficiency and reliability.

ADVANTAGES FOR THE PUBLIC:

- Reduced concentration of intermediaries and infrastructure.
- Less circulation of personal health information.
- Local management of data.

ADVANTAGES FOR HEALTH CARE PROVIDERS:

- Have the entire record including addition and deletion of information with a copy of all transactions by the customer, not just the payment information.
- Offer services that greatly improve the patient's life - the features of management, of accounting and tax reporting, of contracting, interactions with administrations, etc.
- For business associates, elimination of most of the administration, IT and legal work that distracts from their business and increases their vulnerability to bigger competitors.
- Become the single-point-of-security for the patient. All the log-in information managed via the relationship with the health care provider or "covered entity."
- Respond better to societal security concerns by routing data pipelines through banks.

Usually Ricardian blockchain contracts are presented in articles and presentations without a full explanation of how they function because most

people do not want to get into the nitty-gritty of all the technical details.[59] Instead, users are given general explanations of what functions fit into a smart contract now, such as loan agreements, real estate sale, or trade financing.[60] This waters down potential benefits of blockchain and what it can provide to the legal and healthcare sectors. Because, realistically, blockchain smart contracts can work for almost any contract. Most importantly, this approach of explaining contracts hinders the understanding that blockchain is ever evolving, which could change different legal implications of online agreements and how lawyers and courts will deal with them in the future.[61]

This problem with smart contracts has not gone unnoticed.[62] The potential benefits of blockchain-based recordation of contracts should not be underestimated, because the potential for it to become how we record all contracts in the future is strong.[63] However, as long as efforts to model contract formation (by federal regulation, state legislation, or common law) and the transformation of technology remain disconnected, the inconsistency of where the agreement is located on a website (Clickwrap or Browsewrap) will persist.

WHERE IS THIS ALL GOING?

Eris Industries and R3 (both giant coalitions of banks) were early proponents of integrating the recordation of legal prose with the execution of smart contracts.[64] Both of these platforms can capture legal prose and parameters and create executable smart contracts.[65] These two platforms appear to recognize the value of supporting blockchain-based contracting.[66]

I think these FinTech blockchain-based solutions want to get rid of banks acting as a conduit entirely. I believe that if a blockchain-based solution is adhered to by a central bank, it will greatly accelerate this theory because it means more efficiency. The issues, discussed by the Deputy Governor of the Bank of England are:

> [If] distributed ledger technology could provide a more efficient way for private sector firms to deliver payments and settle securities, why not apply it to the core of the payments system itself? . . . The great promise of distributed ledgers for central banks is their potential to enhance resilience. Distributing the ledger means multiple copies of the system. It can continue to operate if parts get knocked out. That removes the single

59. *See* Brent Miller, *Smart Contracts and the Role of Lawyers (Part 2) - About "Code is Law",* BIG LAW KM (Oct. 22, 2016), http://biglawkm.com/2016/10/22/smart-contracts-and-the-role-of-lawyers-part-2-about-code-is-law/.

60. *Id*.

61. *Id*.

62. *Id*.

63. *Id*.

64. *See*, *supra*, note 52.

65. *Id*.

66. *Id*.

point of failure risk inherent in a centralized system. [67]

Putting aside the financial applications of blockchain, as discussed earlier, this technology offers a more secure and flexible alternative to methods of healthcare data transfer. Instead of multiple sets of records for each patient, there will be a single set of records. As a patient's different providers prescribe medication, the prescriptions would become part of the chain. Efficiency and reliability would be increased. But what does this mean for Clickwrap and Browsewrap? It means that eventually they will become obsolete and will not be essential in doing business online because I think that distributed ledger technology is a much more efficient and reliable means of contracting for all parties included. Issues arising on where the actual agreement is and how visible it is will be nonissues since the blockchain ledger offers better management of "signature." Which allows for more informed and fair consents/notice, since the consumer will have to create his or her own contract before using the site or mdevice app.

PART III

The following language is often interlaced into the terms and conditions of most websites regardless of whether they are using Clickwrap or Browsewrap, "Company X may, without telling you, immediately cancel or limit your access to your Company X accounts, certain Company X services and any associated email addresses…" The removal or deletion of an online account erases a person's online identity. Online identities can take time to create and often hold significant value to their owner.[68] At a different level, some companies allow different types of its services to share details about the user.[69] An example of this is Google announcing that under its 2012 privacy policy, which applies across Google services, consumer data will be shared among these services.[70]

In an official statement, Google stated, "Our new privacy policy makes it clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience."[71]

Only Chrome, Google Wallet, and Google Books are not included in the new data-sharing move, and will maintain their own policies.[72] This

---

67. *Deputy Governor: Bank of England Considering Issuing Currency Using a Distributed Ledger,* RED CHALK (2017), http://www.redchalk.com/feature/deputy-governor-bank-of-england-considering-issuing-currency-using-a-distributed-ledger/.

68. Devon S. Connor-Green, *Blockchain in Healthcare Data,*21 U.S.F. INTELL. PROP. & TECH. L.J. 2 181, 184 (2017).

69. *Id*.

70. *See* Hayley Tsukayama, *FAQ: Google's new privacy policy*, THE WASHINGTON POST (Jan. 24, 2012), https://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQArw8GOQ_story.html.

71. Alma Whitten, *Updating our privacy policies and terms of service,* GOOGLE OFFICIAL BLOG, (Jan. 24, 2012), https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

72. *See* Tsukayama, *supra* note 70.

means Google will use data that a user creates like contact details, posts, and photos. Google will also record users' internet activities such as one's habits on YouTube and one's geolocation. Google will basically know where their users' are and what they are doing on their devices.[73]

The issue arises when corporations like Google circumvent hurdles of current regulation. Which undermines current market norms. To explain the legal significance of gaps in regulation the current health care data IT infrastructure and how it is regulated under HIPAA will be used as an example in addition to some case law that has arisen based on gaps of regulation.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Health data is regulated by the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which was amended on January 17, 2013, when the federal Department of Health and Human Services ("HHS"), Office for Civil Rights ("OCR"), issued the long-anticipated final omnibus amendments to the Privacy, Security and Enforcement Rules (the "HIPAA Rules") under the Health Insurance Portability and Accountability Act ("HIPAA"), as directed pursuant to the Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted as part of the American Recovery and Reinvestment Act of 2009.[74]

The 2013 Amendments included a number of changes to the HIPAA Rules,[75] including the expansion of the definition of a business associate to include their subcontractors that handle protected health information ("PHI")[76]; a lower threshold for determining whether a breach has occurred for reporting purposes[77]; and restrictions on "marketing" activities and the "sale" of Personal Health Information (PHI).[78] Business associates are now directly subject to HIPAA with respect to the Security Rule.

COVERED ENTITY

HIPAA only applies to "covered entities" and their "business associates" a covered entity includes: health plans, health care clearinghouses health care providers who conduct certain financial and administrative transactions electronically.[79] These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.[80]

---

73. *See generally* Whitten, *supra* note 71.

74. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY OF 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 [hereinafter HIPAA].

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. *Covered Entities and Business Associates* U.S. DEPT. OF HEALTH & HUMAN SERV. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html?language=es.

80. HIPAA, *supra* note 36.

BUSINESS ASSOCIATES

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.[81] A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. Business associate functions and activities include: claims processing or administration; data analysis processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.[82]

HIPAA PRIVACY RULE

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.[83] The Privacy Rule does not extend to data held by non-covered entities, and to health information about an individual that has been de-identified according to criteria in the HIPAA Privacy Rule.[84] Because of this, there is little understanding of how non-covered entities sharing of de-identified information impacts individuals' privacy, and whether states should regulate, the roles the states have taken in fighting these gaps will be discussed later in part IV.

SECURITY RULE

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity or its business associates.[85] The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[86] The HIPAA Security Rule applies to electronic PHI that is created, received, maintained or transmitted by a covered entity.[87] The 2013 Amendments expanded the scope of the Security Rule to business associates and their contractors. Business associates,

81. C.F.R. § 160.103 (2017) (defining "business associate").

82. *Id.*

83. *Summary of HIPAA Privacy Rule,* U.S. DEPT. OF HEALTH & HUMAN SERV. *(July 26, 2013)*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.

84. *Id.*

85. *Summary of HIPAA Security Rule,* U.S. DEPT. OF HEALTH & HUMAN SERV. *(July 26, 2013)*, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/.

86. *Id.*

87. *Id.*

including their subcontractors that handle PHI, must enter into Business associates agreements that require the business associates to comply with the Security Rule.[88]

Thus, only covered entities or their 3rd party business associates who help create the applications on the mdevices usually will be covered by both HIPAA rules.[89] And the law does not give the Department of Health and Human Services (HHS) the authority to regulate other types of private businesses or public agencies through HIPAA and its amendments.[90] Ironically, most companies that are creating content for mdevices cannot be considered a health care provider or their business associate and will not be covered by these rules. But, by allowing third party non-covered entities to manage personal health data without any regulation only weakens current security measures and puts sensitive information in hacker's hands. Given that there has been a rise of 27% in cyber breaches at federal agencies between 2013 and 2015, and that there is 17.6 million individual cyber breaches in 2014 alone.[91]

Non-covered entities take many forms, however in today's application driven society the use of mHealth technologies is rapidly increasing.[92] mHealth technology allows individuals to monitor daily activities and record vital signs or other biometric data, which is the discussion of part IV, outside of equipment in the doctor's office. These technologies give individuals the ability to become more engaged and aware of their health and serve as an alternative means of collecting and exchanging health information.[93] However, these technologies present privacy issues as most of them are outside of HIPAA's Privacy and Security Rules scope. "Twenty-seven percent of Internet users and twenty percent of adults have tracked their weight, diet, exercise routine, symptoms, or another health indicator online."[94]

CASE LAW: FITBIT FITNESS TRACKERS

A consumer class action suit was filed against Fitbit. That suit alleged that Fitbit's heart rate monitoring system on the Charge HR and Surge models "were dangerously inaccurate and posed serious health risks to users."[95] The plaintiffs alleged that Fitbit's fitness watches "do not and cannot consistently and accurately record wearers' heart rates" during

88. *Id.*

89. *Id.*

90. Connor-Green, *supra* note 68, at 105, 106.

91. Office of Mgmt. & Budget, Exec. Office of the President, M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (2017).

92. U.S. Dep't of Health and Human Serv., *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, HEALTH IT (June 17, 2016), *available at* https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

93. *Id.*

94. *Id.* at 10.

95. McLellan v. Fitbit, Inc., No. 3:16-cv-00036-JD, 2017 U.S. Dist. LEXIS 168370 (N.D. Cal., Oct. 11, 2017).

exercise.[96] The lawsuit alleges that the heart rate monitoring device is faulty when a person is exercising which can lead to a heart attack or death.[97] Fitbit's advertising material claims that PurePulse Trackers use LED lights to detect changes in capillary blood volume in order to "measure heart rate automatically and continuously."[98] Fitbit denies any wrongdoing and has stated that their device is not a medical device and therefore cannot be treated as such.[99] On January 9, 2017, Fitbit urged the judge to compel arbitration.[100]

In another class action, named plaintiffs James Brickman and Margaret Clingman allege that defendant Fitbit misled consumers about the functionality of sleep tracking on its wearable devices.[101] In an amended complaint, the plaintiffs accused Fitbit of violating California and Florida law by falsely claiming that its premium devices can track how long users sleep, the quality of their sleep and the time they wake up.[102] The suit alleges that consumers who bought Fitbit's sleep-tracking-equipped products paid at least $30 more than they would have paid for the basic Fitbit Zip, which does not purport to measure sleep.[103] The court denied Fitbit's motions to dismiss and compelled Fitbit to answer to the complaint.[104]

In 2014, yet another class action lawsuit was filed against Fitbit Inc.,[105] accusing the company of failing to warn about the potential health consequences posed by its popular Fitbit Force, including the risk of skin irritation, rashes and burns.[106] The case shows that there have been over 900,000 (or 1.7% of all Fitbit force users) instances of people developing skin irritations, such as rash, hives, boils or open sores on their wrist as a result of wearing the band. Fitbit has announced a voluntary recall of the Fitbit Force due to reports of skin irritation.

SEXUAL ACTIVITY TRACKED BY FITBIT SHOWS UP IN GOOGLE SEARCH RESULTS

In July 2011, several Fitbit users had their sexual activity exposed to the world. A simple Google search turned up results showing when the users' sexual activity began, how long the activity lasted, and sometimes very detailed description of the sexual activity because of the title of the activity was posted as well. The problem was not that Fitbit was recording sexual activity. Instead users were choosing to record the activity themselves. But, instead the default privacy and sharing settings for the Fitbit was set to public

96. *Id*.
97. *Id*.
98. *Id*.
99. *Id*.
100. *Id*.
101. Brickman v. Fitbit, Inc., No. 15-cv-02077-JD, 2016 U.S. Dist. LEXIS 150125, at *2 (N.D. Cal., July 15, 2016).
102. *Id.* at *3.
103. *Id.* at *4.
104. *Id.* at *12.
105. Jim Spivey v. Fitbit, Inc., Case No. 37-2014-00007109, SUPER. CT. OF CAL. (San Diego).
106. *Id*.

instead of private. So, if the user didn't unclick the default setting, it allowed user profiles to be found in search results (Google, Bing, etc).[107] This meant that many Fitbit users probably failed to realize that their sexual activity was online and available until they saw the story about this break on the news. Fitbit after realizing the mistake moved to set the default sharing setting to "private," which hid its users' activity tracking details on its website, and contacted various search engines to have the data removed from search results.[108]

APPLE AND NIKE FITNESS TRACKERS

In 2013, a false advertisement class action lawsuit was filed against Nike Inc. and Apple Inc.,[109] alleging these companies violated consumer protection laws and warranty obligations by making misleading statements about the iOS-exclusive Nike+ FuelBand products.[110] The lawsuit against their fitness trackers stated that the heart rate monitor and calorie-tracking monitors were inaccurate and potentially dangerous to the health of the individuals wearing the devices. Nike and Apple deny all liability in regard to the Nike+ FuelBand false advertisement allegations, but have decided to settle the case in order to avoid the uncertainty and cost of further litigation. They settled the case in 2015 by giving customers a partial refund in the form of $15 or $25 gift cards.[111]

WEARABLE FITNESS DEVICES IN DISCOVERY

The first well-publicized use of a fitness device in a legal proceeding took place in Canada in November 2014.[112] The plaintiff in that case used the data from her Fitbit fitness tracker to prove that she had experienced a decline in physical activity after sustaining an injury in a car accident.

In March of 2015, police used data from a wearable fitness device to support charges of false report to law enforcement, false alarms to public safety, and tampering with evidence. The police used evidence from the defendant's wearable fitness device to contradict a statement made by the defendant.[113] During the time that the defendant alleged that she was

107. Leena Rao, *Sexual Activity Tracked by Fitbit Shows Up in Google Search Results*, TECH CRUNCH (Jul. 3, 2011), https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/.

108. Kashmir Hill, *Fitbit Moves Quickly After Users' Sex Stats Exposed*, FORBES (July 5, 2011), https://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/.

109. Levin v. Nike Inc. et al., Case No. BC509363 (2013), SUPER. CT. OF CAL. (Los Angeles).

110. Karina Basso, *Nike+ Fuelband Class Action Settlement,* TOP CLASS ACTIONS (July 28, 2015), https://topclassactions.com/lawsuit-settlements/closed-settlements/79799-nike-fuelband-class-action-settlement/.

111. *Id*.

112. Carol Michel & Rick Sager, *Wearable Fitness Devices: A New Frontier in Discovery*, LAW 360 (March 28, 2016), https://www.law360.com/articles/775527/wearable-fitness-devices-a-new-frontier-in-discovery.

113. *Id.*

sleeping, her wearable fitness tracker showed that she was awake and active. The police used this information to bolster their claim that this was the time that she was staging a fake crime scene. The case law has shown that in establishing case law on this matter, courts must strike a balance between the benefits of technology and people's expectation of privacy.

PART IV

Like mdevices and third party non-covered entities collection and use of consumer data, HIPAA is also silent on collection and use of biometric data by non-covered entities[114] Up to this date, only Illinois and Texas have statutes in force that in particular focus on the collection and use of biometric data. Alaska, Connecticut, Montana, New Hampshire, and Washington all have pending state legislation.[115]

ILLINOIS

Enacted in 2008, Illinois' Biometric Information Privacy Act (BIPA), requires companies to obtain consent as a threshold before collecting, capturing, or purchasing a person's:

> [B]iometric identifier or biometric information, unless it first: (1) informs the subject . . . in writing that . . . biometric information is being collected or stored; (2) informs subject . . . in writing of the specific purpose and length of term for which . . . biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the . . . biometric information . . . .[116]

BIPA defines "written release" as "informed written consent."[117] Consent must also be obtained when the business plans to "disclose" or "disseminate" the individual's biometric information.[118]

BIPA makes possessors of biometric information create privacy policies that are made available to the public, which should set out a retention schedule and guidelines for permanently destroying the data.[119] BIPA also, provides that biometric information must be destroyed either when the purpose for collecting the biometric information "has been satisfied" or within three years of the "individual's last interaction with the private entity" – whichever occurs first.[120]

BIPA prohibits businesses from profiting in any form from an individual's biometric information.[121] Businesses should consider this when

---

114. HIPAA, *supra,* note 36.

115. *See States Continue to Fill Gaps in Privacy Legislation: Illinois Biometric Law Gains Traction and Serves as Model for Other States*, JDSUPRA (April 19, 2017), http://www.jdsupra.com/legalnews/states-continue-to-fill-gaps-in-privacy-56861/.

116. 740 ILL. COMP. STAT. ANN. 14/15(b) (West 2008).

117. 740 ILL. COMP. STAT. ANN. 14/10 (West 2008).

118. 740 ILL. COMP. STAT. ANN. 14/15(d)(1) (West 2008).

119. 740 ILL. COMP. STAT. ANN. 14/15(a) (West 2008).

120. *Id.*

121. 740 ILL. COMP. STAT. ANN. 14/15(c) (West 2008).

determining how they are going to use biometric information, and what policies they will put in place to comply with BIPA. BIPA creates a private right of action for "any person aggrieved" by a violation of the statute and provides for statutory damages of $1,000 (or actual damages, whichever is greater) for a negligent violation, or $5,000 (or actual damages, whichever is greater) for an intentional or reckless violation, as well as injunctive relief, while a prevailing party may also collect attorney's fees.[122]

TEXAS

Texas has a similar statute addressing biometric data, the Capture or Use of Biometric Identifier Act (CUBI). However, unlike BIPA, which creates a private right of action, in Texas only the Texas Attorney General can bring an action to enforce. CUBI, like BIPA, describes "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[123] CIBA requires informed consent to capture any biometric information but does not specify the form that the notice and consent must take.[124] But the Texas statute's scope is limited to biometric information used for a "commercial purpose."[125] Thus, businesses could make the argument that if biometric information is not directly used to obtain a profit or other tangible benefit, this statute should not apply.

CUBI precludes organization that possesses biometric data captured for commercial purposes from selling, leasing, or disclosing the information unless one of the following exemption scenario exist: (1) the individual consents to the disclosure for purposes of identifying him in the event of his disappearance or death; (2) the disclosure completes an authorized financial transaction; (3) the disclosure is required or permitted under a state or federal statute; or (4) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.[126]

Any collected or stored biometric data must be destroyed within a "reasonable time," and no later than one year after the date when the purpose for collecting the biometric data expires.[127]

The potential exposure for statutory violations of CUBI is significant, with civil penalties of up to $25,000 for each violation.[128] However, there is no private right of action under CUBI. Instead, only the Texas Attorney General can recover civil penalties under the statute. The Texas statute requires collectors to store, transmit and protect biometric data at least as

122. 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).
123. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2017).
124. TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).
125. TEX. BUS. & COM. CODE ANN. § 503.001(c) (West 2017).
126. TEX. BUS. & COM. CODE ANN. § 503.001(c)(1) (West 2017).
127. TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2017).
128. TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2017).

protectively as it would other confidential information it possesses, if biometric information applies.[129]

CONCLUSION

Every jurisdiction should update their rules governing the specifications for wearable devices. This would be a temporary solution, as more extensive legislation like HIPAA is developed. The most reliable change would be to broaden the language defining covered entities and their business associates in HIPAA to include all developers of medical health technologies. Third party vendors that do deal with private consumer health data should not be allowed to deal in this information in secret.

Blockchain's distributed data characteristics are well suited to maintaining the privacy and security of medical records. Implementing blockchain technology into all national health care data contracts will vastly increase how we can connect to our data and manage it accordingly. Not only that but it will get rid of the complications of Clickwrap and Browsewrap.

The technology already is being implemented. The Bill and Melinda Gates Foundation awarded the technology company Factom a large grant for deploying blockchain for medical records.[130] Individual medical records, secured by blockchain, provide a way to ensure uptime and access.[131] Professor Reza Dibadj of the University of San Francisco School Of Law, had this to say regarding legal compatibility issues with the technology:

> Blockchain could redefine the concept of a patient's medical record. State laws focus on provider's responsibility to store and maintain patient records for a fixed time period. Medical providers are under legal duties to produce records to patients. These legal duties may not match the realities of blockchain technology in action. The shift will be from medical records to medical data, and the law is ill prepared for this transformation.[132]

Hopefully, within the next decade, enough medical providers and legal establishments are taking advantage of blockchain technology and that enough case law will exist to provide precedent on how data from this new technology should be used and permitted in litigation.

---

129. TEX. BUS. & COM. CODE ANN. § 503.001(c)(2) (West 2017).

130. Mike Miliard, *Gates Foundation Gives Factom a Grant to Deploy Blockchain for Medical Records*, HEALTHCARE IT NEWS (Nov. 21, 2016), http://www.healthcareitnews.com/news/gates-foundation-gives-factom-grant-deploy-blockchain-medical-records?mkt_tok=eyJpIjoiTjJZM05qUXdaV0V6TlRkbSIsInQiOiJFeVg0UWZ0VDFja1dBcmdjNXZ3XC9KSktBRUR3SXVFOGhFTmo3XC9aaUd3dEE2WHBlUndpZm15eFwvcGZpSmxJVHdDTVFjclN6V2VYSEZmRUdcL1FCKzg4YlVDc0NiK0tjOFM1dnRvQkZDQlwvZ2MwPSJ9.

131. *Id.*

132. Michael Sacopulos, *Blockchain: The Future of Health Data*, DIAGNOSTIC IMAGING (April 11, 2017), http://www.diagnosticimaging.com/blog/blockchain-future-health-data.