RESEARCH MEMORANDUM: WEARABLE TECHNOLOGY

To: **Belmont Inn of Court**
From: **Wearable Technology Team**
Date: **February 6, 2017**

Question Presented: What legal issues arise from a litigation perspective by the rise in the use of wearable technology.

Short Answer: While there are a myriad of issues, the most common ones appear to be the discoverability of such technology, the privacy implications involved, and how the law will evolve to adapt to the technology that is outpacing it.

FACTUAL BACKGROUND

Wearable technology is here to stay. With a sales growth of 200 percent from just 2013 to 2014, what was then an already 3.5 billion dollar industry is expected to increase in sales five-fold by 2019. While they go by many names – Fitbit, Apple Watch, Basis Peak, Bellabeat LEAF, Jawbone Up2, Garmin Vivosmart,' Mio Fuse – wearable devices ("wearables") are remarkably singular in purpose: to be real-time, twenty-four/seven personal trackers of virtually every aspect of our lives. These devices are capable of compiling an unprecedented amount of fitness and activity data generated by users. They capture data in areas as diverse as one's heart rate, stress level, blood pressure, brain activity, calories burned, respiration rate, body temperature, sleep patterns, running speed, mileage ran, glucose levels, and number of steps taken. Additionally, the location of users can be tracked, with some wearables being able to pinpoint a user's location to within a few millimeters. One researcher at the University of California at San Diego likened the functional capabilities of a wearable to that of a car, stating "we know exactly how much gas we have, the engine temperature, how fast we are going . . . [what we are] doing is creating a dashboard for [the] body."[1]

While there are clear health and medical benefits of having this technology literally at our fingertips, there also comes with it a risk: infringements upon our right to privacy. A more interconnected world, which provides us with a host of conveniences we could once only dream of, has the potential for abuse in litigation and otherwise. As an emerging technology and field of study, wearables are largely uncharted territory in the law. One thing is clear: there is no consensus on how to best address the difficult issues lawyers and courts will face in the near future as wearables become widely used and the information they collect is sought by adverse parties.

[1] Nicole Chauriye, Note and Comment, *Wearable Devices as Admissible Evidence: Technology is Killing our Opportunities to Lie*, 24 Cath. U. J. L. & Tech. 495, 1 n.36 (2014).

LEGAL ISSUES

I. DISCOVERABILITY

A. Pertinent Discovery Principles

There are a host of applicable discovery procedures under the Tennessee Rules of Civil Procedure that implicate the discoverability of wearable technology. The Federal Rules of Civil Procedure raise additional issues. These rules cover the scope of discovery and ways to compel the production of tangibles and electronically stored information. Pertinent rules include:

1. Tennessee Rule of Civil Procedure 26.01: Rule 26.01 states: "Parties may obtain discovery by one or more of the following methods: depositions upon oral examination or written questions; written interrogatories; production of documents or things or permission to enter upon land or other property for inspection and other purposes; physical and mental examinations; and, requests for admission." Note that the rule indicates "one or more of the following methods." This is significant because one method alone might not cut it; rather, a combination of methods might be needed given the complexity and scope of wearable technology.

2. Tennessee Rule of Civil Procedure 26.02: Rule 26.02 imposes limitations on the extent to which parties can obtain discovery to avoid unfettered fishing expeditions. For example, subsection (1) of the rule provides that "[p]arties may obtain discovery regarding any matter, *not privileged*, which is *relevant* to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party." (Emphasis added.)

As for reasonableness, the rule provides that "[i]t is not ground for objection that the information sought will be admissible at the trial if the information sought appears *reasonably* calculated to lead to the discovery of admissible evidence." (Emphasis added.) However, this degree of latitude is checked by whether "(i) the discovery sought is *unreasonably* cumulative or duplicative or is obtainable from some other source that is more convenient, less burdensome or less expensive." (Emphasis added.) Thus, should the method of discovery place an undue burden on the opposing party, the court may find that a chosen method needs restrictions or should be abandoned altogether.

As it pertains to wearables, consideration should be given to the rule's discussion of electronically stored information: "A party need not provide discovery of electronically stored information from sources that the party identifies as *not reasonably* accessible because of undue burden or cost." (Emphasis added.) A description of what constitutes "electronically stored information" is not provided, only a reference to unspecified "sources" which is not defined in the rule.

It is important to note too that the burden rests with the party from whom discovery is sought to establish an undue burden or cost should a party choose to withhold requested material. Specifically, the rule states that "[o]n motion to compel discovery . . . the party from whom

discovery is sought must show that the information is not reasonably accessible because of undue burden and cost."

Further, under subsection (5) of the rule, which primarily concerns privileged material, the burden rests with the party exercising this protection to expressly state its claim of privilege:

> When a party withholds information otherwise discoverable under the rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege protection.

Parties may also find it necessary to rely on Rule 26.02(4)(A)(ii), which permits a party to depose a party's expert witness expected to testify at trial. This part of the rule can come into play when the parties or court would benefit from having a technical expert explain how a particular wearable device works or, on a broader scale, to breakdown the process by which information is transmitted to a device's servers and/or network. Wearables range in complexity and their operation is not always intuitive, especially for the technologically challenged.

3. Tennessee Rule of Civil Procedure 34: Rule 34 concerns the production of documents "and things." As with discovery in general, the scope of what can be requested is broad but not unlimited, encompassing both tangible items and electronically stored information,

> including writings, drawings, graphs, charts, photographs, sound recordings, images, phono-records, *and other data and data compilations stored in any medium* from which information can be obtained either directly or, if necessary, after translation by the respondent into a reasonably usable form.

Tenn. R. Civ. P. 34.01 (emphasis added).

4. Tennessee Rule of Civil Procedure 34.02: Rule 34.02 provides that "[i]f a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is *ordinarily maintained* or in a form or forms that are *reasonably usable*."

5. Tennessee Rule of Civil Procedure 37.01: Rule 37.01 permits a party to move for an order compelling discovery. The motion can make the request on a number of grounds including, among other things, a party's failure to answer a question "propounded or submitted under Rules 30 or 31 . . . or a party['s] fail[ure] to answer an interrogatory submitted under Rule 33."

6. Tennessee Rule of Civil Procedure 37.06: Rule 37.06 addresses electronically stored information, which will undoubtedly be a source of contention for litigants involved in a case relying on evidence derived from the use of wearable technology. Rule 37.06(1) provides as follows:

> If a party fails to provide electronically stored information and a motion to compel discovery is filed, a judge should first determine whether the material sought is subject to production under the applicable standard of discovery. If the requested information is subject to production, a judge should then weigh the benefits to the requesting party against the burden and expense of the discovery for the responding party.

Relevant factors identified in the rule include -

> the ease of accessing the requested information; the total cost of production compared to the amount in controversy; the materiality of the information to the requesting party; the availability of the information from other sources; the complexity of the case and the importance of the issues addressed; the need to protect privilege, proprietary, or confidential information, including trade secrets; whether the information or software needed to access the requested information is proprietary or constitutes confidential business information; the breadth of the request, including whether a subset (e.g., by date, author, recipient, or through use of a key-term search or other selection criteria) or representative sample of the contested electronically stored information can be provided initially to determine whether production of additional such information is warranted; the relative ability of each party to control costs and its incentive to do so; the resources of each party compared to the total cost of production; whether the requesting party has offered to pay some or all of the costs of identifying, reviewing, and producing the information; whether the electronically stored information is stored in a way that makes it more costly or burdensome to access than is reasonably warranted by legitimate personal, business, or other non-litigation-related reasons; and whether the responding party has deleted, discarded or erased electronic information after litigation was commenced or after the responding party was aware that litigation was probable.

It is important to note that the requested information is "subject to production under the applicable standard of discovery." Another consideration is the burden and expense of obtaining the information and whether the information is available from other sources. Last, one should consider whether the information is privileged, proprietary, or confidential. Here is where privacy concerns can arise.

7. Federal Rules of Civil Procedure: The Federal Rules provide additional areas for consideration. First, it is important to evaluate whether wearable technology should be disclosed as a part of a party's initial disclosures under Rule 26(a)(1) of the Federal Rules of Civil Procedure. Second, the standard for discoverability has recently been amended by the federal rules under Rule 26(b) so that the state rules no longer mirror the federal rules. Per Fed. R. Civ. P. 26(b)(1), technology is discoverable if it is "nonprivileged matter that is relevant to any party's claim of defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant

information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." The remaining Federal Rules of Civil Procedure do not differ materially from the Tennessee Rules of Civil Procedure; however Rule 37.06 of the Tennessee Rules contains extensive language not found in its federal counterpart.

B. The Courts

There are very few cases addressing issues regarding wearable technology, such as privacy concerns, and whether information obtained from wearables is, or should be, discoverable, much less its admissibility in court. Below is a summary of some instructive cases:

1. *Riley v. California*, 134 S. Ct. 2473 (2014): In this criminal case involving the search of cell phone data by police officers without a warrant, the Supreme Court held that neither the interest in protecting officers' safety nor the interest in preventing destruction of evidence justified the warrantless search of cell phone data. This holding could be used to draw parallels between the search of digital content found on cell phones and that which can be obtained from wearables. "The crux of whether or not *Riley* should be applied to require warrants to search smart activity trackers is whether the data they contain is similarly private to that of cellphones and thus merits Fourth Amendment protection."[2]

To illustrate, heart rate data is arguably inherently private and likely to be protected by the Fourth Amendment because "[e]ven more so than GPS data, heart rate data has the potential to enable inferences that reveal deeply personal information, such as sleep patterns, sexual activity, physical exertion, and general health, especially when the data is available second by second."[3] However, with the host of other data that wearables track, how to apply the warrant requirement in the face of new technology is unclear. "Court readings of *Riley* are clearly inconsistent and will only breed confusion as courts are forced to apply *Riley* to new and varying smart devices. Courts need a singular standard by which to assess the warrant requirements for all smart devices."[4]

Justice Alito, in his concurring opinion in *Riley*, offered his thoughts on how to rectify technological advancement and its accompanying privacy concerns:

> In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.

---

[2] Katharine Saphner, Note: *You Should Be Free to Talk the Talk and Walk the Walk: Applying Riley v. California to Smart Activity Trackers*, 100 Minn. L. Rev. 1689, 1711 (2016).
[3] *Id.* at 1715.

[4] *Id.* at 1705.

As Justice Alito observed, the judiciary is ill-suited to respond to such changes. Legislatures, on the other hand, are more responsive, being the better forum for presenting these difficult, policy-driven issues.

2. *U.S. v. Graham*, 824 F.3d 421 (4th Cir. 2015): Despite the holding in *Riley*, when conducting an analysis under the lens of the "third-party doctrine" as to whether the warrantless search of cell phone data was constitutional, the Fourth Circuit held that such information did not require a warrant. The Court found that the Supreme Court precedent has consistently held that "an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to [a] third part[y].'"[5] The "voluntary" nature of the data disclosure was deemed an inherent part of the business relationship between the defendants and the service provider and the analysis by the Court could easily apply to wearable technology.

The Court recognized a disconnect between advancing technology and the need for responsive legislation. "[I]n the face of rapidly advancing technology, courts must 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted'" By the same token, "technological advances also do not give individuals a Fourth Amendment right to conceal information that otherwise would not have been private."[6] The Court further stated, "[i]It is human nature, I recognize, to want it all. But a world of total privacy and perfect security no longer exists, if indeed it ever did. We face a hard future of hard tradeoffs and compromises, as life and privacy come simultaneously under siege."[7]

3. *Commonwealth v. Risley:* In a Pennsylvania case, a rape claimant was ordered to serve two years of probation and complete 100 hours of community service for making a false allegation she had been sexually assaulted one night while sleeping in her employer's residence. When authorities arrived, they noticed a Fitbit on the floor and requested that it be submitted as evidence. The claimant complied by providing Fitbit login information and turning over the device. After further investigation, authorities determined that the claimant was in fact not asleep the night of her alleged assault but awake and walking around the residence as corroborated by data obtained from the Fitbit. The device also showed that activity consistent with her supposed movements existed up until the time she called 911. Based on these findings, the claimant was charged with tampering with evidence and making a false report.[8]

4. *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (Sup. Ct. N.Y. 2010): While this case did not involve wearables, the following quote is instructive on the potential attitude of the courts when

[5] *Graham*, 824 F.3d at 425.

[6] *Id.* at 436.

[7] *Id.*

[8] Jacob Gersham, *Prosecutors Say Fitibit Device Exposed Fibbing in Rape Case*, Law Blog, The Wall Street Journal (Apr. 21, 2016, 1:53 PM ET), http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case.

dealing with discoverability of this type of technology: "[W]hen Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."[9] Certainly, however, distinctions can be drawn between wearable technology and social media.

5. Personal injury litigation: In 2014, a Canadian law firm represented a woman who was injured in an accident. To demonstrate the extent of her injuries, the woman's lawyers used her Fitbit to measure her activity levels after the accident. The plaintiff's lawyers planned to use physical activity data from the Fitbit tracker at trial to show how her lifestyle had been severely impacted by her injuries. The results showed that because of her accident, her activity level was less than that of an average woman of her age and profession. This is believed to be the first case where a plaintiff's lawyer was able to use the physical activity data from a client's Fitbit tracker to show the impact on one's lifestyle resulting from injuries. *See* 24 Cath. U. J. L. & Tech. 495.

6. Expert Testimony: Perhaps one way to present such technology in a lawsuit is to use an expert in this field as the foundation to present the data. To do so, the wearable technology data relied on by the expert would have to be "of a type reasonably relied upon by experts in the particular field in forming opinions or inferences" and the data "need not be admissible in evidence", provided that the data does not "indicate lack of trustworthiness." Tenn. R. Evid. 703; *see also* Fed. R. Evid. 703. Whether such data could ultimately be used in courts in this state will require overcoming several legal and factual hurdles.

II. DATA SECURITY AND PRIVACY

Inherent in the intersection of wearable technology and litigation is the issue of privacy and data security. The first line of defense against privacy violations are the mechanisms that companies have adopted for combating them. Note that "[h]ealth and financial data are more risky than certain other types of personal information because they are more sought after."[10]

A. Network Security

In a comparative analysis of the data transmissions of eight leading activity trackers, Open Effect, a Canadian technology think-tank, determined that data in the categories of (1)

[9] *Romano*, 907 N.Y.S.2d at 656.

[10] Zainab Hussain, *Weary of Wearables: IP, Privacy, and Data Security Concerns*, p. 2. Law Practice Today (2016), http://www. lawpracticetoday.org/article/weary-of-wearables-ip-privacy-and-data-security-concerns/

basic personal information, (2) fitness data, (3) location information, (4) social information, and (5) technical device data were the most commonly shared types of data from the use of wearables. While the use of a secure HTTPS connection between user and server was effective at deterring a user's tampering with his or her own fitness data for five of the eight wearables that were tested, it did not safeguard the device from end users abusing the service, which can spell disaster for users if their data were to get into the wrong hands.[11]

"Data sold, stolen or leaked through a data breach, to third parties such as insurance providers, for example, could allow insurers to quote [a policyholder] higher rates for health insurance, or even cancel her policy, without her knowing how or why, or even that the Insurer was able to access he wearable device data."[12] Fitbit, in particular, encrypts its user-generated fitness data on the device itself before being transmitted to its servers. "The servers then presumably decrypt the data into a structured format and store it. The [mobile] application then downloads the data from the server for display."[13] However, wearables manufactured by Bellabeat, Jawbone, and Withings do not provide the same level of security, arguably enabling researchers to submit fraudulent data. "These companies do not seem to use mechanisms to verify that generated fitness data originates from the wearable device itself."[14]

B. Privacy Policies

Companies' privacy policies are relatively easy to access from their websites. "Many of these privacy policies, however, fail to explicitly break down and differentiate between data collected in the course of providing information via the company's website, to collecting fitness data with wearables, to processing that data using mobile device applications."[15] Aside from Apple, Withings, and Xiaomi, the other wearable companies studied by Open Effect reserve the right to sell user data in the event of a bankruptcy.[16] Additionally, Basis and Fitbit are permitted to sell de-identified data, and all of the companies can "choose to, or be compelled to" release information to authorities.[17]

---

[11] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, p. 32. Open Effect Report (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[12] Zainab Hussain, *Weary of Wearables: IP, Privacy, and Data Security Concerns*, p. 2. Law Practice Today (2016), http://www. lawpracticetoday.org/article/weary-of-wearables-ip-privacy-and-data-security-concerns/

[13] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, p. 33. Open Effect Report (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[14] *Id.* at 36.

[15] *Id.*

[16] *Id.* at 46.

[17] *Id.*

It should be noted that complaints, and potential litigation, rely upon what information wearable companies have retained:

> As such, whether there is a statute limiting access to data, or if data is inaccessible following the deletion of an account, is important for collecting evidence needed to file a complaint. Several companies, including Apple, Basis, Bellabeat, and Mio, do not disclose for how long they retain personally identifiable information associated with their wearable products in their privacy policies or terms of service/use documents.[18]

C. Best Practices

Officials in the wearable technology industry are turning to best-practice models as a means of avoiding government regulation which could prove to be "stifling" to innovation.[19] Federal Trade Commission Chair Edith Ramirez advises that:

> Companies [need] to 'bake' privacy into their devices or applications from the start. The strategy would be to push companies to build devices with privacy elements such as additional passwords and encryption; to reduce the amount of data that devices collect and store; to make data as anonymous as possible; and to increase company transparency with additional consumer notices on devices – particularly if companies plan to share the data with third parties – and the ability to consent or not to data collection.[20]

Consistent with this approach, Open Effect recommends utilizing transit-level encryption for all internet communications.[21]

III. POTENTIAL REGULATORY ISSUES

There is always the likelihood that wearables will be regulated at some point. It is clear that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is not triggered by wearables because health professionals are not involved, but it may one day be amended to address privacy concerns deriving from the protection of health data. The Stored

---

[18] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, p. 43. Open Effect Report (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[19] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. Mo. B. 76, 77 (2016).

[20] *Id.* at 78.

[21] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, p. 64. Open Effect Report (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

Communications Act (SCA),[22] a statute within the Electronic Communication Privacy Act of 1986 (ECPA), provides a more specific framework for regulating the transmission of information stored electronically. The intersection of HIPAA and the SCA, and what their respective provisions did not contemplate with the emergence of wearable technology, is worth considering.

At the state level, Tennessee's Patient's Privacy Protections Act could, it seems, come into play when a party seeks to discover tracked information, particularly the confidentiality provisions of Tennessee Code Annotated § 68-11-1503.

Conclusion: Wearable technology will continue to evolve quickly, posing steep challenges for a legal system anchored in tradition and generally slow to adapt.

[22] 18 U.S.C. §§ 2701-2712 (2012).