Title: Technology Trends in International IP: Practitioner's Insight Into Foreign Trends and Global Treaties

Date: March 17, 2016

Time: 11:00 PM to 12:15 PM

Moderator

Cecilia Sanabria
Associate
Finnegan
cecilia.sanabria@Finnegan.com

Panelists

Catherine Romero
Senior Attorney
Microsoft
cromero@microsoft.com

Darrell G. Mottley
Principal Shareholder
Banner & Witcoff
dmottley@bannerwitcoff.com

Tab 1 – Biographies or CVs

Cecilia Sanabria

Associate
Profile | Articles

Cecilia Sanabria's practice involves patent litigation, patent prosecution, and client counseling. Currently, she devotes most of her practice to litigating patents before U.S. district courts and the U.S. International Trade Commission (ITC). Her litigation experience spans the pre-trial, discovery, trial, and post-trial phases of litigation. She manages fact discovery, drafts motions and legal briefs, and works with fact and expert witnesses. In addition to her litigation practice, Ms. Sanabria works with various aspects of patent prosecution, including *inter partes* and *ex parte* reexamination requests.

Ms. Sanabria also devotes a portion of her time to pro bono matters. She worked on landlord-tenant disputes through the firm's work with the DC Bar, and has represented criminal defendants in the Virginia Supreme Court.

While obtaining her degree, Ms. Sanabria worked for General Electric and was involved in engineering design in the area of aircraft engines as well as technical sales of medical systems. She was also a mentor in a program designed to promote academic success among minority engineering students. During law school, Ms. Sanabria worked at Finnegan as a summer associate and a law clerk.

Highlights

- *Kaneka Corp. v. SKPI* (C.D. Cal.). Defends SKPI against charges of patent infringement on its polyimide films.
- *U.S. Philips Corp. v. Hewlett-Packard Co.* (E.D. Va.). Represented Philips in asserting MPEG technology patents against Hewlett-Packard's media player and computer products.
- *HTC Corp. v. Apple, Inc.* (D. Del.), and *Certain Portable Electronic Devices and Related Software*, 337-TA-721 (ITC). Represented HTC in enforcing its patent rights against infringing iPhones, iPads, and iPods.
- *Certain Portable Electronic Devices*, 337-TA-721 (ITC). Represented HTC against Apple in a high-profile investigation involving power management and graphical user interfaces of mobile devices.

Professional Recognition

- Recognized as a Washington, D.C. "Rising Star" in Intellectual Property Litigation, *Super Lawyers*, 2014-2015.
- Received the 2003 Hispanic Engineer National Achievement Awards Corporation Scholarship from Northrop Grumman.
- Served as vice-president of the Society of Hispanic Professional Engineers, 2003-2004.

Professional Activities

- American Bar Association
- Hispanic National Bar Association (chair, IP section, 2016; chair, Awards committee, 2014; co-chair, CLE planning committee, 2014)
- Hispanic Bar Association of the District of Columbia

Select Publications

- Coauthor. "Litigation at the International Trade Commission: Considerations if the Complainant Relies on a Licensing Domestic Industry," *Imp & Exp Executive Magazine*, May 2012.

Catherine Romero

Catherine is a Senior Attorney at Microsoft supporting O365 and Outlook engineering teams. Catherine started her legal career as a business, corporate, and securities attorney at Perkins Coie in Seattle, and has since worked at various in-house legal departments. She is a member of the Latina Commission of the Hispanic National Bar Association. Prior to her legal career, Catherine spent 7 years as a Boeing engineer where she worked on a number of DOD projects.

Darrell G. Mottley

Attorney

Darrell G. Mottley is a principal shareholder of Banner & Witcoff, and the past president of the D.C. Bar. Mr. Mottley provides strategic counseling in intellectual property protection related to patent and trademark matters, including procurement, opinions, licensing and litigation. Mr. Mottley's intellectual property practice includes complex technologies in a variety of fields such as telecommunications, internet-related technology, computer-gaming, medical devices, semiconductors, mechanical technologies, and electro-mechanical technologies.

Recently, Mr. Mottley advised a Fortune 500 company on an anti-counterfeiting project which included opinion analysis and scope and patent identification in a global anti-counterfeiting action using design/registrations. Mr. Mottley has advised clients on intellectual property matters in multi-million dollar venture capital transactions. He has successfully represented clients and obtained U.S. utility and design patents through the U.S. Patent and Trademark Office (USPTO), and the firm successfully enforced the patents to protect the core businesses of clients. He has successfully represented clients before the USPTO Board of Appeals and Patent Interference. Mr. Mottley has advised global companies on patent clearance and prosecution in cooperation with local country counsel in countries such as Singapore, Taiwan, Malaysia, Thailand, China, Hong Kong, Europe, Mexico, Russia, Brazil, Peru, and South Africa.

Throughout his career Mr. Mottley has worked as an engineer, a project manager, engineering chief for the AAI Corporation, U.S. Army Belvoir Research and Engineering Development Center, and the National Oceanic and Atmospheric Administration. He has worked in diverse fields such as network communications, data center design and construction, advanced composite materials, military electronics, and military aircraft logistics and maintenance.

Mr. Mottley earned a Bachelors of Science in Engineering Science and Mechanics in 1987 and his Masters of Business Administration from the Virginia Polytechnic Institute and State University in 1994 with a concentration in corporate finance and management science. He earned his Juris Doctor degree, *with honors*, in 2000 from The George Washington University, where he also served as an editor on the student editorial board of the*ABA Public Contract Law Journal*. He had an article published in the journal concerning information technology in the Federal Government.

Mr. Mottley is the former Chair of the District of Columbia Bar's Council on Sections. He also served as Vice-chair of, Division IV of ABA Section of Intellectual Property Law. Mr. Mottley is registered to practice before the United States Patent and Trademark Office and is a member of the National Bar Association concentrating on intellectual property law. He is also a Fellow of the American Bar Foundation, the premier U.S. socio-legal research institute.

Mr. Mottley completed a four year term on the Industrial Advisory Council at the College of Engineering at Virginia Tech. In this capacity he assisted with the recruitment, retention, and development of students in engineering, focusing on under-represented students from diverse backgrounds.

Mr. Mottley is an adjunct professor at The George Washington University Law School teaching classes in design law. Mr. Mottley previously lectured on patent law at Howard University Law School. Mr. Mottley is a contributing author to the Thomson Reuters published book, Navigating Fashion Law: Leading Lawyers on Exploring the Trends, Cases, and Strategies of Fashion Law, in which he authored the section "The Tools for Protecting Fashion Law Clients." He is also a contributing author to the ABA published book, Annual Review of Intellectual Property Law Developments, in which he authored the section "Design Patent Infringement – Egyptian Goddess." He currently serves as editor-in-chief of the ABA's *Landslide* magazine.

Tab 2 – Course Materials (articles, publications, other materials)

http://www.fastcompany.com/3044662/sector-forecasting/what-latin-america-will-look-like-in-2020

What Latin America Will Look Like In 2020

Leaders from some of the Most Innovative Companies in Latin America offer their predictions on what the future of the region holds.

We asked the world's Most Innovative Companies in Latin America to map out how business will change there in the next five years.
Here's what they had to say.

Tech Will Give The Taxi Industry A Much-Needed Facelift

Car-hailing apps are ubiquitous in the U.S., but big data and the sharing economy have yet to catch on in Latin America. Andrés Gutierrez—cofounder of the popular taxi-hailing app Tappsi—says change isn't far down the road. Since it can still be dangerous to hail a taxi in many capital cities in Latin America, safety will be key. "Brands that already have consumer trust will start making inroads into this new transportation feature," says Gutierrez. Tappsi screens every driver and provides a secure chat interface that allows drivers and passengers to communicate without sharing phone numbers, and lets users' family and friends track their taxis. And by analyzing user data, Tappsi can recognize which passengers have similar destinations—allowing them to pair up and improve efficiency in an industry where cabs are only utilized for 60 percent of the time they spend on the road.

Plus, Gutierrez says that the varied cultural landscape of Latin America means that successful travel apps will have to think locally rather than globally. "While a passenger hailing a cab in São Paolo might be looking to find the quickest cab, a passenger in Lima is surely hustling the price with the driver—not to mention how a passenger in Quito is not looking for price or quickness, but just that the driver is legit and he is not going to be robbed," says Gutierrez. "That's how diverse the consumer needs are from market to market."

Millennials Will Usher In A New Era Of Digital Payments

Due to spiraling inflation and widespread distrust in banks, many people in Argentina still keep cash under their mattress. Add to this the stiff financial regulations in Latin America and the huge amount of paper money still in circulation there, and Latin America may seem like the last place for a financial innovation boom.

But Banco Galicia is trying to give consumer finance in the region a digital makeover. "Millennials have new ways of socializing and relating to banks," says Emiliano Porciani, a marketing manager at Banco Galicia. "They think that banking is one of the sectors with more disruption opportunities. In order to acquire and retain these customers, banks will constantly have to innovate through new technologies."

Take, for example, Galicia MOVE—Argentina's first all-digital banking services suite that's targeted to university students. Launched last spring, the service counts 35,000 clients across Argentina, and allows users to send and receive money, track their spending, and more. Porciani predicts that mobile payment systems already permeating the North American financial space, like Square and Apple Pay, will accelerate innovation in Latin America, forcing big banks to finally adapt.

The Private Sector Will Help Overhaul Some Government Functions

Luis Arnal's Mexico City-based consultancy Insitum has worked magic for more than 50 public and private-sector companies across Latin America, spotlighting where design thinking and improved processes could better impact citizen experience. (Insitum is responsible for nearly 200 innovation projects in the region.) From that unique vantage point, Arnal sees an opportunity for the private sector to correct some of Latin American's governmental shortcomings.

"Due to lousy, bureaucratic, and corrupt governments, private companies and entrepreneurs will take over a lot of government functions, sparking huge opportunities to profit from a vast population that won't mind paying to get the service they deserve—mostly in health care, education, energy, and finance," he says.

Arnal also predicts Latin American governments will finally take steps toward forming a single trade bloc that includes Venezuela and Cuba, allowing Latin America to compete with other regions. This includes a pan-legalization of marijuana to reduce criminal activity and provide better conditions for medium-sized businesses to prosper, he says.

Smartphone Growth Will Encourage New Mobile And Digital Currency Technology

Latin America has the fastest rate of smartphone adoption in the world, and the first computer many in the region will ever have access to will be a smartphone. As the suburbs of megacities like Mexico City and Buenos Aires continue to grow, Tambero founder and CEO Eddie Rodríguez von der Becke says a newfound access to technology and the Internet could cause the popularity of local apps to skyrocket.

Latin America has the fastest rate of smartphone adoption in the world.

"These new suburbanites will have access to technology and Internet through mobile but will not be accustomed to the formal economy or traditional financial systems," he says. "[Streaming services] PopCorn Time and Cuevana were local piracy inventions which became massive because the majority of the population does not have credit cards to pay for Netflix or iTunes, or they were considered expensive in relation to the local incomes." Plus, a new generation of mobile users could create an ideal environment for a new digital currency, he says.

Meanwhile, smartphones will help even the most remote farmers connect with their land. Developed in rural Argentina, Tambero is the first free, web-based global system for agriculture. Used in more than 150 countries, it helps farmers everywhere improve yields by enabling them to manage animals and see comparative reports through a phone or tablet. While farms in Brazil and Argentina act as "massive production machines," von der Becke says poor, small-scale farmers in Bolivia and Ecuador will be able to harness new ideas and techniques from the Internet as well as access a new market for delivering their goods.

Latin America Could Be The Next Hot Spot For Social Innovation

Latin America is ready for its own Occupy movement, says Jose Manuel Moller—the founder of Algramo, a startup that makes affordable staples like rice and detergent available to poor, remote communities in Chile via vending machines. A large millennial population and a trend toward consumer empowerment in the region are about to create fireworks for Latin America, he says.

Millions of Latin American families live on less than $5 a day, which has contributed to a culture of intense effort and resilience. That combined with the momentum created by a new startup mentality in the region will

lead to thousands of local solutions to everyday challenges that are able to scale up, predicts Moller.

"Because LatAm is one of the most unequal places in the world, we have stopped believing in the solutions that only look for economic growth, and we are aware that it's time to find solutions to the inequality problems," he says. "This will change the idea that the maximization of shareholder utilities is the priority, and will put first the solution of social and environmental problems." As a result, Moller sees plenty of B corporations and social-good companies cropping up in the region's near future.

http://www.businessinsider.com/tech-trends-changing-the-world-2014-4

GOLDMAN: These 7 Tech Trends Are Changing The World

The list includes seven "concurrent revolutions within the technology space." Disruptive technology is having a huge impact on global businesses and the economy that we can't ignore.

We've highlighted the seven key tech trends they think are about to impact the global economy:

E-Commerce platforms: The growth of e-commerce will see "the first real digital generation come into its own." Online shopping platforms will start competing for a larger share of the retail market. Digital commerce is expected to gain traction with annual growth hitting about 17% in the next three years.

REUTERS/China Daily

Healthcare technology: Doctors have been able to use technology to detect diseases as varied as cancer to other infectious diseases early. Goldman points to Massachusetts-Based Hologic which has a "3-D mammographic technology" that allows doctors to detect minuscule cancers that they previously wouldn't have been able to detect.

Goldman Sachs

Cloud computing: The shift to cloud computing has been a gamechanger in both the storage and sharing of vast quantities of data and has even led to new business models. "The most successful cloud computing application companies are the ones that are enabling us to engage with our day job the same way we engage as consumers on the

internet," said George Lee co-head of the technology, media and telecommunications group at Goldman.

Goldman Sachs

An unprecedented growth rate: Tech companies are some of the world's biggest companies with businesses that have the most impact. "They're growing faster than many of the companies that came before them, and arrive at critical decision points more quickly."

Goldman Sachs

Monetization of mobile: Smartphone and tablet sales now outpace PCs and laptops. And companies cognizant of this are trying to capitalize on mobile "whether in mobile payments, mobile content, location-based services or the explosion of valuable data generated by the use of mobile devices." There's a lot of scope for companies to monetize this.

REUTERS/Bobby Yip

Pervasiveness of technology: It isn't just the growth of technology, it's also the "pervasiveness." Over 4 billion people have cellphones and in the next five to ten years nearly all of them will have access to some form of computing technology. This is changing how people consume and how much they consume. And technology has the habit of building on itself so the growth and pervasiveness will continue.

Goldman Sachs

The next wave of disruption: 3-D printing, big data solutions (in which data is collected from different devices and information is consolidated), and software-defined networking (SDN) are the next wave of disruptive technologies to watch for. "3-D printing will drive greater customization, reduce costs for complex designs and lower overhead on short-run parts," according to Goldman. Meanwhile, "SDN liberates

networking from expensive hardware, making it easier and cheaper for technology administrators to respond to changing business needs."

7 No. 5 Landslide 59
Landslide
May/June, 2015
Department

I²P GROUP NEWS

Samson Helfgott[a1]

A number of interesting items have come up with respect to the I²P Group (International Intellectual Property Group), which are of interest to the entire membership.

EPO INCREASES AGREEMENTS ON PPH

The Patent Prosecution Highway program (PPH) has grown over the last few years, and as of January 6, 2014, a Global Patent Prosecution Highway Program has been developed. Participating in the Global PPH are the following offices: Australia (IP Australia), Austrian Patent Office (APO), Canadian Intellectual Property Office (CIPO), Danish Patent and Trademark Office (DKPTO), Finnish Patent and Registration Office (PRH), Hungarian Intellectual Property Office (HIPO), Icelandic Patent Office (IPO), Israel Patent Office (ILPO), Japan Patent Office (JPO), Korean Intellectual Property Office (KIPO), Nordic Patent Institute (NPI), Norwegian Industrial Property Office (NIPO), Portuguese Institute of Industrial Property (INPI), Russian Federal Service for Intellectual Property (ROSPATENT), Intellectual Property Office of Singapore (IPOS), Spanish Patent and Trademark Office (SPTO), Swedish Patent and Registration Office (PRV), United Kingdom Intellectual Property Office (UKIPO), and United States Patent and Trademark Office (USPTO).

Under the Global PPH, allowable claims either resulting from a national examination or a PCT search report from one of these countries can be used in another of these countries in order to accelerate prosecution of similar claims in that other country. In addition to accelerating the time, it has been found that allowance rates, number of office actions, and first action allowances are all better when using the PPH. This is an expected result since the claims have already passed prosecution in an earlier country.

In addition to the Global PPH, the IP5 has also established an IP5 PPH project. The IP5 members include China, United States, Japan, Europe, and Korea. All of the IP5 countries, except Europe, are also members of the Global PPH. The EPO has not joined the Global PPH. However, they have instituted bilateral agreements with individual counties.

At present, in additional to the IP5 countries, the EPO has established bilateral agreements with Canada, Israel, Mexico, and Singapore and have indicated that they plan to continue entering additional bilateral agreements with other patent offices.

INDIA SEEKS COMMENTS ON A NEW DRAFT IP POLICY

The Indian Department of Intellectual Policy and Promotion (DIPP) published their first draft of a new IP policy. The draft mostly addressed recommendations concerning structure of the court system, and did not address the sensitive IP issues such as compulsory licensing of pharmaceutical products and the unique patentability requirement of the Indian patents act requiring that a pharmaceutical provide “enhanced therapeutic efficiency”.

In connection with the court system that was addressed, the draft recommended setting up intellectual property sections in four of the state high courts and designating one district court in each district as an intellectual property court. It also suggested setting up regional sections of the Intellectual Property Appellate Board in cities where the Patent Office already has branches. ***60**Recommendations also included modernizing and streamlining IP administration. In keeping with the rapid growth and diversity of intellectual property users and services, it also suggested greater responsibilities and increases to the workload at the Patent Office.

So far, the recommendations have received mixed reviews. Many view these recommendations as inadequate in improving the Indian patent laws. Furthermore, as part of the draft it reiterated that the Indian Patent Law conformed to the World Trade Organization's Agreement On Trade Related Aspects of Intellectual Property Rights (TRIPs), and many challenge whether the Indian laws are actually compliant with the TRIPs requirement.

JPO TO REVISE OPPOSITION SYSTEM

As part of a government stress on economic growth, Japan passed an amendment to the patent law in 2014 to implement changes in the opposition system. These amendments will take effect in 2015. Currently, the system requires an opponent of a patent to file paper documents as well as make oral arguments.

Under the revised system, a third party observation system is introduced. Objections by third parties can be filed at any time and can be raised anonymously. These observations can address issues of double patenting, patentability, new matter, clarity, and enablement. The new opposition procedure will also be available to anyone, but they must be identified and it must be submitted within six months from grant. The same grounds for third party observations are also available in the opposition procedure. Typically, a decision will be made within one year.

The current invalidation trial system will remain, however only a party in interest will be able to file for such invalidation and must be identified. It is available throughout the life of the patent. A decision will typically be made within nine months from the request.

In all of these systems, however, the patentee can amend the claims as such practice is quite liberal in Japan during these procedures.

IP5 ISSUE PATENT STATISTICS FOR 2013

The IP5 offices including US, Europe, Japan, Korea and China released their statistics for 2013. Overall, patent applications were up by 11% with a total of 2.1 million filed. The offices issued 4% more patents than in the previous year. As of December 2012, 8.5 million patents were in force throughout the world, an 8% increase over the previous year. The U.S. is still in the lead with over 2.2 million of those patents.

The number of patents in force at the end of 2012 among the IP5 were:

Jurisdiction	Number	Present
United States	2,239,231	26.2
Europe	2,135,765	25.0
Japan	1,694,435	19.8
China	875,385	10.2
South Korea	738,312	8.6
Other	858,959	10.1

Patent office fillings for the IP5, together with an indication of how many of those were filed by domestic applicants within that country, were:

Office	Filings	Domestic	Percent
United States	571,612	287,831	50.4
Europe	147,869	73,420	49.7
Japan	328,436	271,731	82.7
China	825,136	535,315	82.0
South Korea	204,589	159,978	78.2

SECOND MEETING OF GLOBAL DOSSIER TASK FORCE

The **Global Dossier** is a joint project of the IP5 Patent Offices and the IP5 Industry Group through a joint **Global Dossier** Task Force. The first meeting of the task force took place in The Hague, in January 2013. At that time it was agreed to provide an integrated online portal/user interface between users and all participating offices. It would allow access to available information about all applications and patents in the participating offices and to utilize the electronic services of the individual offices. Each country will have a portal through which users in that country would gain access into the patent databases of the other participating offices and ultimately permit two-way communication with the patent participating office.

All the information of each patent office will remain on its own server. It will only be accessed from each portal country. While initially it would include the databases of all IP5 countries, ultimately it will provide access to WIPO-CASE and other countries that want to participate.

Two parts were envisioned. The first was referred to as the passive part providing global file accessibility. The other would be the active part for one portal document submission, such as cross fillings of patent applications.

The passive part has actually been implemented in all five patent offices. Currently, it is being used by examiners. It is envisioned that it will be available to the public during 2015 in each of the five patent offices.

In using the passive part, one enters a patent number of any patent family and then get the list of the entire patent family including the patents issued and pending applications. The user can then select any country participating in the **Global Dossier**. The user is able to view a table of contents of all the documents in the file wrapper of that application in that country. Upon selecting one particular document, the user may access the actual content of the document, for example an Office Action, and it is provided in both the original language and machine translated into the language of the country whose portal is being accessed.

The second meeting of the **Global Dossier** Task Force met at the end of January 2015 in Suzhou, China. Discussions took place on how to proceed to ***61*** further enhance the currently developed passive part, as well what new areas should be addressed in moving toward implementation of the active part.

It was agreed that the ultimate goal should be cross filing of applications. However, along the way there are smaller projects that can be achieved. One project agreed upon was the proof of concept project. Essentially, a single uploading of a document would be tested to be sure this capability can be achieved. The project selected was change of address. The proof of concept will require filing a change of address in one patent office, and then being able to upload it into the individual corresponding family members of any of the other five patent offices. This will require addressing issues including security, translations, uniform requirements, establishing handshaking between the participating offices, and many other issues. It is envisioned that once this proof of concept can be achieved, it can then be built upon for uploading other documents, including ultimately cross-filing.

Other projects that were agreed upon include adding the patent legal status into the current system. This would provide information on where the application is in its prosecution, and whether the patent is alive.

Further projects include standardizing and unifying applicants' names for consistency in all of the IP5 offices, as well as providing all of the documents uploaded in XML so that they can be easily searched and both the applicants as well as the patent offices can use it to formulate final documents. An additional project is an alerting system to alert applicants when a change of status take place, such as an office action issuing on a maintenance fee being due.

Various patent offices will address these projects individually and share the information developed with the other patent offices. Also, users will be involved during the development of each of these projects.

FAST TRACK TRADEMARK PROTECTION IN EUROPE

The Office for Harmonization in the Internal Market (OHIM) which handles European trademarks, has provided a new system to obtain trademark protection in an expedited manner. Under the new fast-track system, the regular processing time of a community trademark can be reduced by about

one-half. As a result, the applications which participate in the new system will be published sooner for opposition purposes. Should there be no incoming oppositions, faster registration will take place on these applications. In order to be applicable for the fast-track system, one must pay the official fees immediately. Another requirement is adherence to the terms of good and services already accepted by OHIM. There is no official fee for requesting the fast track system.

TRILATERIAL PATENT OFFICES MET IN JAPAN

The Heads of the Trilateral Patent Offices, including the United States, Japan, and the European Patent Office (EPO), met in Yokohama, Japan, at the beginning of March 2015. Prior to their meeting, the Industry Trilateral Organizations including American Intellectual Property Law Association (AIPLA), IPO, Business Europe, and Japan Intellectual Property Association (JIPA) held their meeting and thereafter joined with the heads of the patent offices for a joint meeting.

The discussions focused on the issues of substantive patent harmonization, as well as the results of IP5 work on the Patent Harmonization Expert Panel (PHEP). The IP5 had agreed that the PHEP would address three issues, namely unity of invention, citation of prior art, and written description requirements. Under the leadership of the EPO, the unity of invention topic has been discussed and information from the five patent offices was obtained. The EPO is now coming up with a set of practices so that unity of invention in all of the five patent offices should be more uniformly decided.

The issue of citation of prior art is being worked on by the USPTO and KIPO. They are also gathering information on the ability of the five patent offices to address the issue of citation of prior art through electronic means by using various existing data bases to alleviate the burden on applicants.

The JPO is addressing the written description requirement and have undertaken a number of studies including addressing a glossary of terminology used by the various patent offices in connection with sufficiency of disclosure, written description, clarity and similar terminology. JIPA is also conducting various studies and analyses of the rejections in various patent offices to determine the relationship of clarity and other rejections by the various patent offices.

All of the patent offices will be providing their recommendations to the deputy heads meeting of the IP5 at the end of March, and that group then will decide on the final plan to be presented to the Heads of the IP5 Patent Offices during their meeting scheduled at the end of May in China.

With respect to substantive patent law harmonization, the industry trilateral indicated that they are working on a paper which should be available within a few weeks. The paper will list discussion points on harmonization of six topics, including description of prior art, conflicting applications, grace period, prior users rights, 18-month publication, and unity of invention. The paper will discuss the various issues, indicating where consensus has been achieved, and in those areas still open for discussion, will provide various alternative approaches and analyses of those approaches.

It is hoped that once that paper is completed, it will be passed to other organizations including the Industry IP5, the B+ Countries, the IP5 Heads, as well as other national and international bar

associations. The purpose will be to get further input on the open topics for discussion and to see if further consensus can be achieved on those open topics.
It was felt that progress thus far achieved by the Industry Trilateral was quite significant in light of the fact harmonization has been a difficult and challenging goal for many, many decades.

a1
Samson Helfgott is a partner with Katten Muchin Rosenman LLP in New York. He has practiced for more than 30 years in domestic and international patent, trademark, and copyright matters.

Copyright Battles over the Internet of Things

Franklin S. Graves

Franklin S. Graves is general counsel and business and legal affairs at Naxos of America, Inc., in Nashville, Tennessee. He specializes in entertainment, technology, and business law. He can be reached at fgraves@naxosusa.com.

At this year's Consumer Electronic Show (CES), the Internet of Things took over the show floors—pushing aside 3D printers and pulling ears away from Sony's hi-res audio initiative. The Internet of Things, or IoT abbreviated, is all about leveraging wireless technologies to enhance the interoperability of objects and items that consumers interact with on a daily basis. Single-use coffee pods, cars, smoke detectors, power outlets, light bulbs, and more have all been transformed to communicate both with each other on a local level and across networks miles apart.

The Internet of Things Explained

IoT has become a popular buzzword across multiple industries. The basic concept for IoT started as an opportunity to turn everyday objects into "smart" objects capable of improving operability and efficiency. The objects are programmed to communicate by way of wireless standards as common as Wi-Fi and Bluetooth or as specialized as protocols such as ZigBee and Z-Wave.[1]

Objects can be transformed into "smart" objects through two basic methods: by design and by retrofitting. IoT objects by design are manufactured with built-in wireless communication capabilities. A common example is the Nest thermostat, which not only allows remote control functions but also learns behavioral patterns of its users. Non-IoT objects can be retrofitted by way of adapters or other technological innovations that provide the necessary wireless capabilities. For example, a basic way to transform any non-IoT electrical object in the home, such as a lamp, into an IoT object would be to purchase an adapter for the power outlet that allows basic controls—i.e., "on" or "off"—by way of an in-home Wi-Fi network or radio signals.

Maintaining Corporate Control

Over time, IoT has encountered a variety of high and low points throughout its implementation. Most of the issues have stemmed from corporations seeking to use IoT technologies as a way of maintaining control over the devices they sell. The IoT provides opportunity to utilize copyright law to lock down consumer devices and hardware in often divergent efforts for maintaining functionality and safety of products and continued financial gain once a product is in the consumer's hands. Utilizing copyright law provides protection of computer code and other IoT devices that, when combined with end-user license agreements, can prevent tampering and reverse engineering by consumers and third parties. The result places consumers in a situation where they are unable to "tinker" with their cars or brew their own choice coffees.

Through public backlash and steady profit losses, numerous corporations have been forced to retreat in their decisions to utilize copyright laws in an effort to lock down ecosystems.

Coffee: Green Mountain

It's hard to find a home or office that doesn't have a single-serve coffee or espresso pod brewing machine, more commonly known by the brand name Keurig or K-Cup. Up until September 2012, when several of the key patents owned by Green Mountain Coffee Roasters for the single-cup brewing pods[2] expired, Keurig was the only authorized outlet for K-Cup supplies. The market for single-serve pods changed dramatically, as forecasted, with competitors able to sell their own version of coffee pods that are compatible with the Keurig brewing systems.

The company's response to the issues faced through competition included a new line of Keurig 2.0 machines launched in August 2014. The 2.0 machines were implanted with IoT technology that would require a special seal printed on top of the K-Cup pod, which was only available on authorized Keurig-produced pods. Users would be given an error message on their machine if an unapproved pod, even the eco-friendly reusable pods previously sold by Keurig, were inserted into a new machine.

Backlash to the new systems ranged from negative customer reviews to antitrust lawsuits[3] to competing brands offering hacks to bypass the technology. Keurig recently announced a return of the My K-Cup pod to allow customers the option of brewing their own coffee; however, it still leaves open the question of how non-Keurig branded pods are supposed to interact with the system—if at all.

Printer Ink: Lexmark

Printers are practically given away when purchasing a new computer system because large amounts of money come from the sale of replacement ink cartridges. As a result, corporations needed a way to make sure that revenue stream didn't run out due to third-party cartridges and toner refill services undercutting the cost of a brand-new cartridge from the manufacturer. For Lexmark, one option included implementing chip technology that would reject anything but "valid" cartridges manufactured by Lexmark. The technological measure was reverse-engineered by Static Control, a company which then sold the necessary chips to third-party toner manufacturers for use in the Lexmark printers.

A powerful Digital Millennium Copyright Act (DMCA) case in 2004, *Lexmark v. Static Control* answered the question of whether circumventing the protection measure put in place by Lexmark violated copyright law.[4] Section 1201 of the DMCA makes illegal the act of circumventing technological protections designed to prevent the unlawful copying of a work, with a few limited exceptions.[5] The Sixth Circuit ultimately held that reverse-engineering did not violate the DMCA in this particular case.

Convenience is another powerful tool printer manufacturers can use in bypassing third-party cartridge makers. Harnessing the power of IoT, a printer can be programmed to automatically order replacement toner from the manufacturer before running out, or perhaps even order from its owner's retail store of choice.

Vehicle and Equipment Manufacturers

In 2014, the U.S. Copyright Office published a list of proposed exemptions to the DMCA's anticircumvention of copyright protection measures.[6] The list of exemptions is updated once every three years, including periods of public comment on any proposed exemptions. One of those exemptions, Proposed Class 21, would make it legal for anyone to repair, diagnose, or modify the software running on their vehicle or equipment. General Motors LLC[7] and Deere & Company (known by the brand name John Deere)[8] submitted comments against the exemptions, citing safety and policy concerns further supported by their copyright interests in the vehicle and equipment software. Software systems in cars power the transformation into the IoT category by integrating smarter and more connected features, but are also the source of contention within the automotive industry.

The foundation of the argument for automakers is that ownership rights to a vehicle do not extend to the software, but rather the purchase includes only a license to that software. As John Deere stated, "the vehicle owner receives an implied license for the life of the vehicle to operate the vehicle."[9] Manufacturers are able to exhibit more control over how the end consumer can interact with the software by granting a restrictive license to the software on the vehicle. A license that doesn't grant the right to use or inspect the code can prevent owners, in addition to third parties, from lawfully servicing, modifying, or diagnosing their vehicle. In 2014, Ford Motor Company filed a lawsuit against the diagnostic equipment company Autel US Inc., claiming Autel hacked into a Ford diagnostic software system in order to improve the Autel diagnostic system.[10]

This level of control could limit consumers' choice of where to have their vehicle serviced, and allow the manufacturer to control variables such as how much the services cost to perform and where the services can be performed. The other side of the argument in favor of these controls is that safety measures and regulatory requirements are often met during the initial manufacturing process. The concern would be that third-party modifications could seriously interfere with and create unknown variables to vehicle systems designed to operate in a specific manner. However, if the automotive sector of the IoT is ever going to have an open environment, then automakers will need to implement technologies that promote and enhance interoperability.

What Does Copyright Mean for IoT Going Forward?

The current IoT landscape is being driven the way of operating systems—such as Windows, Apple OS X, or Linux. Some IoT products will communicate within one standard, while others may only communicate within another. Both Google and Apple have released home automation standards, Brillo/Weave[11] and HomeKit[12] respectively, and each are currently only compatible within each company's ecosystem. Additionally, both technology companies launched separate automotive operating systems, Apple's CarPlay[13] and Google's Android Auto.[14] The IoT marketplace is headed toward a segmentation based upon consumers' decision as to which ecosystem in which they invest.

Intellectual property laws will continue to play important roles as more complex items are introduced and everyday lives begin incorporating the IoT technologies. Consumers and companies alike will seek ways in which one "thing" can interoperate with another "thing." Licensing of key technologies and a basic level of cooperation among competing brands will become a prerequisite to achieving a goal of openness and interoperability for the future of the IoT.

Endnotes

1. For more, see Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things*, RE/CODE (Jan. 15, 2015), http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/.

1 U.S. Patent No. 5,325,765 (filed Sept. 16, 1992).

2 *In re* Keurig Green Mountain Single-Serve Coffee Antitrust Litig., No. 1:14-md-02542-VSB

(S.D.N.Y. June 5, 2014).

1 Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

2 17 U.S.C. § 1201.

6. U.S. Copyright Office, 1201 Rulemaking: List of Proposed Classes 2014, http://copyright.gov/1201/docs/list-proposed-classes-1201.pdf.

7. Comments of General Motors LLC, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07 (U.S. Copyright Office Mar. 27, 2015),

http://copyright.gov/1201/2015/comments-032715/class%2021/General_Motors_Class21_1201_2014.pdf.

8. Long Comment Regarding a Proposed Exemption under 17 U.S.C. 2101, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07 (U.S. Copyright Office Mar. 27, 2015), http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf.

- *Id.* at 5–6.
- Ford Motor Co. v. Autel US Inc., No. 2:14cv13760 (E.D. Mich. Sept. 29, 2014).

11. *Project Brillo*, GOOGLE DEVELOPERS, https://developers.google.com/brillo/ (last updated June 3, 2015).

1 *HomeKit*, APPLE DEVELOPER, https://developer.apple.com/homekit/ (last visited Sept. 7, 2015).

2 *Apple CarPlay*, APPLE, http://www.apple.com/ios/carplay/ (last visited Sept. 7, 2015).

3 *Android Auto*, ANDROID, https://www.android.com/auto/ (last visited Sept. 7, 2015).

IoT Big Data: Consumer Wearables Data Privacy and Security

By Katherine E. Britton

Katherine E. Britton has her own practice, is of counsel at Simmons Legal, PPLC, and is an affiliate professor at the University of North Texas Dallas College of Law in Dallas, Texas. Katherine specializes in complex civil litigation, employment and human resources counseling, probate, estate planning, consumer protection, and privacy law matters. Katherine is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals and is admitted to the bars in Illinois, the District of Columbia, and Texas. She can be reached at kebritton1@gmail.com.

> [T]he world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly. . . . The effect is being felt everywhere, from business to science, from gov ernment to the arts. Scientists and computer engineers have coined a new term for the phenome non: "big data."[1]

In the United States, the age of big data is upon us. In 1965, Intel co-founder Gordon Moore predicted that the number of transistors on a computer chip would double every two years while the chip's price would remain constant. "Moore's law" meant consumers could buy the same technology two years later for about the same price. Fifty years later, Moore's prediction has remained remarkably accurate to the point that technology companies have recognized Moore's law as a benchmark they must meet, or fall behind in the market.[2] The wearables market generally follows Moore's law, creating a "mad rush" among companies to bring products to market. Consumers have come to expect technological products to be faster, cheaper, and more compact over time; this expectation has driven trends of rapid growth in computing power, smaller devices, better battery life, ability to connect to the Internet, and reduction in cost.

Ideally, this consumer demand should drive the market; however, the wearables market poses certain intellectual property imperfections pertaining to data privacy. For example, consumers have imperfect information about how companies collect and use personal data. Federal data privacy regulations in the United States focus on following the Fair Information Practice Principles: notice, choice, access, accuracy, data minimization, security, and accountability. Third-hand collected personal data—the data of consumers who do not use wearables but whose data are collected by others' wearables—would not be protected by the Fair Information Practice Principles.

The benefits wearables pose to consumers are considerable, assuming data security and data privacy concerns are addressed. This article explores the existing and developing infrastructure and technological features supporting wearables, the specific data privacy and security concerns wearables pose in the United States commercial sphere in the age of big data, particularly in the healthcare space, and the idea that policymakers should address the data privacy and security concerns posed by wearables because consumers and businesses are unlikely to do so.

IoT Infrastructure Supporting Wearables Might Not Address Data Privacy or Security

IoT Connectivity Is Based on RFID Technologies

Kevin Ashton, one of the founders of the Massachusetts Institute of Technology (MIT) Auto-ID Center, is credited with coining the term "the Internet of Things" (IoT).The term refers to objects embedded with technologies like microchips, sensors, and actuators that often use Internet Protocol (IP) and share data with other machines or software over communications networks. Wearable computing devices, or "wearables," are a subset of IoT. The MIT Auto-ID Center was founded in 1999 with the mission of pioneering a global open standard system for radio-frequency identification (RFID) technologies. By developing RFID technologies, the Center laid the foundation for the many architectures supporting IoT.

RFID technologies use radio waves, microchips, and antennas to identify people, products, and objects automatically. RFID technologies use machine-to-machine (M2M) transmissions, which refer to direct communications between machines such as a microchip and a microchip scanner, a wearable and a third-party application (app), or a wearable and a monitoring hub. M2M transmissions share information without any special configuration or other setup requirements. For example, veterinarians use RFID technology to identify missing microchipped pets. In 2004, the Food and Drug Administration (FDA) approved a similar technology for use on humans.[3] The technology relies on a slender capsule of bioglass imbedded in the skin. That capsule contains a microchip with a unique serial number, and is attached to a tiny antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The capsule's sole function is to store and transmit a unique identification code to a reader. The code can be read with a microchip scanner passed over the skin. The reader converts the radio waves reflected back from the RFID tag into digital information that can be compared to a veterinary or medical database.

IoT Connectivity Relies on Systems That Handle Security Independently

Wearables are subject to cybersecurity attacks. In April 2014, a vulnerability in Internet encryption (named the Heartbleed bug) was so widespread that it affected wearables.[4] The Federal Trade Commission (FTC) held a workshop titled "Internet of Things: Privacy and Security in a Connected World" (FTC Workshop), solicited public comments, and published a staff report in January 2015 summarizing the various viewpoints. When considering how to handle data security, there was widespread agreement among panelists at the FTC Workshop on the need for companies manufacturing IoT devices to incorporate reasonable security measures.[5] These devices, however, also rely on legacy systems that may not be secure.

Sanjay Sarma, one of the MIT Auto-ID Center's founders, described the problem as not IoT themselves but the "pell-mesh rush to build systems in any which way" without regard to a comprehensive security plan.[6] The underlying challenge, Sarma explained, is that even if independent systems were secure, these systems are cobbled together, and "the chain will only be as strong as the weakest link."[7] The soft-ware used for IoT apps also pose a problem for data security because, like the infrastructure, they "are hard to upgrade or improve" and use a "patchwork of legacy systems [such] that it is virtually impossible to replace any one without a wholesale replacement of all."[8]

Exploding Wearables Market Might Not Address Data Privacy or Security

Sensors Embedded in Wearables Allow Them to Gather Huge Amounts of Data

Wearables collect tremendous amounts of data. The technologies surrounding wearables allow that data to be used and analyzed in a variety of ways. Wearables today are embedded with more advanced technologies including microchips, sensors, and actuators. As of 2012, 3.5 billon sensors are already on the market.[9] According to a June 2015 Lux study analyzing patents filed between 2010 and May 2015, 41,301 patents were granted for wearable electronics, and patent applications for wearable electronics are increasing at over 40 percent annually.[10]

Information about a person derived from wearables data such as the time, duration, and proximity of an activity to other tracked individuals combined with demographic information can provide crucial and detailed context to each individual interaction. Data gathered impacts how businesses market their products and how companies recruit talent and motivate their employees. Wearables gather a new class of sensitive data about people: not only who they are, what they do, and who they know, but also how healthy they are, what movements they make, and how well they feel.[11] Heart rate monitors can provide insight into people's excitement and stress levels, and glassware can reveal exactly what they are seeing. Microsoft's health-tracking wearable, Microsoft Band, incorporates exotic sensors like galvanic skin response, the same technology that is used in lie detectors. By adding heart rate and temperature information, it is now possible to make educated guesses on a user's emotional state. There is now a handsfree Tinder app for the Apple Watch that instead of allowing the user to decide consciously on a match by swiping left or right on his or her smartphone, makes the decision using the wearer's heartbeat.[12]

Consumers Demand Wearables

Great Wolf Resorts, owner of 11 water parks in North America, has used RFID wristbands since 2006 that allow the resort company to track users throughout the park and tie their activities and purchases to their names.[13] These wristbands allow users to pay for food and beverages on account and allows them to avoid carrying money or keys on waterslides. In 2013, Walt Disney World introduced a similar vacation management system to provide users with a more customized park experience. Economist Paul Krugman cited the "Varian rule," which provides that the future can be forecasted by examining what the rich have today, supporting the idea that consumers would want resort-like experiences in their daily lives.[14] For example, the super-rich do not wait in line, rather "[t]hey have minions who ensure that there's a car waiting at the curb, that the maître-d escorts them straight to their table, that there's a staff member to hand them their keys and their bags are already in the room. . . . [S]mart wristbands could replicate some of that for the merely affluent."[15]

Companies' Demand for Big Data Is Increasing

The European Commission's new antitrust chief, Margrethe Vestager, described data as the "new currency of the Internet." FTC Chairwoman Edith Ramirez made a similar comment: "Today's currency is data."[16] Apart from consumer goodwill and trust by self-disclosing "we won't collect your data" (asApple CEO Tim Cook has done), there is little incentive for a company not to collect data on consumers using wearables.[17] A 2011 McKinsey report noted that when a competitor fails to use data and business analytics to guide decision making, it suffers competitively.[18]

Data collected by wearables can be analyzed to create highly targeted, individually tailored marketing campaigns. Marketers could derive from raised stress levels, poor sleep, and a combination of other behavior that a romance is in trouble. Wearable data could determine if a user was habitually late for work, largely immobile when at the office, or spent little time with his or her colleagues, and determine such behavior is due to low morale or dissatisfaction with his or her current job.

Analyzing data from wearables in conjunction with other information will allow businesses to deliver messages and services tailored to a particular customer's location, activity, and mood.[19] Recruitment firms could use big data to target dissatisfied workers, and employers can use the same data to implement policy changes.[20] De-identified and aggregated data from wearables reveal otherwise indiscernible patterns and trends in a number of socially beneficial contexts. Medical and epidemiological research, energy conservation, and commercial productivity and efficiency are benefits of using big data.[21] Companies can use aggregated data to have a better idea of consumer demand and develop better products and services.

Companies Innovate Independently without Addressing Data Security

In the rush to bring new wearables to market, companies may not address the data security threats. According to Cisco, by 2019, 24 billion networked devices are expected to come online (compared with 14 billion in 2014). By the end of 2012, 8.7 billion devices were connected to the Internet. That figure is expected to increase to 40 billion by 2020 as cars, refrigerators, ovens, thermostats, medical devices, and others come online.[22]

IoT Innovation and Infrastructure in Healthcare Wearables

Healthcare Wearables Present the Greatest Potential for Consumer Gains

Healthcare wearables contain wireless sensors embedded in the device and worn on the body. M2M technologies and healthcare apps along with healthcare wearables could improve patient outcomes, reduce health expenditures, and allow providers to deliver care in more patient-friendly ways. For example, insulin pumps and blood-pressure cuffs that connect to mobile apps could let people record, track, and monitor their own vital signs without having to go to a doctor's office.[23] Healthcare providers can monitor patients' blood pressures, respiration rates, and a variety of other biometric information remotely and continuously thanks to wearables.

Healthcare wearables engage patients in their own care. A clinical trial of diabetic users of continuous glucose monitors showed an average blood sugar level reduction of two points; to put this finding in perspective, the FDA considers medications that reduce blood sugar by as little as one-half point to be successful.[24] Economist Paul Krugman said that he uses a Fitbit "because the thing spies on me all the time, and therefore doesn't let me lie to myself about my efforts."[25]

Healthcare wearables also help medical providers better understand patient's health and healthcare issues in general. By analyzing continuous data, healthcare providers are better able to spot trends and make better decisions. In the case of continuous glucose monitors, healthcare providers can examine a patient's blood glucose levels throughout the day and over the course of their disease. Examining aggregated data, they can spot trends and better understand diabetes and how it can be controlled.[26]

Healthcare Wearables May Pose Data Security Risks

Security risks of healthcare wearables increase with the degree of human interaction. There is a significant degree of human interaction in telehealth apps. The data captured by healthcare wearables typically flow across short, unlicensed wireless links to a monitoring hub in the patient's home, which then passes the information to the broadband network, routing it to the cloud where analytics continuously monitor a patient's status, notifying a healthcare provider in case of anomalies.[27] Healthcare wearables measure a patient's biometric data; an on-premises healthcare worker or a medical professional can receive the data on the other end of a wireless communications link.

In the hospital setting, medical devices have become the key points of vulnerability within healthcare networks and have been subject to attacks.[28] Medical devices including x-ray equipment, picture archive and communications systems, and blood gas analyzers have been the subject of cybersecurity attacks.[29] These attacks threaten overall hospital operations and the security of patient data. If a hospital, with a fixed infrastructure, cannot keep its medical devices secure, it is highly likely that consumers will be more vulnerable to cybersecurity attacks.

Does Government Regulation Address the Data Privacy and Security Concerns Wearables Pose?

U.S. Data Privacy Regulations Follow Fair Information Practice Principles

Even if a company follows Fair Information Practice Principles and a consumer trusts a particular company with his or her data today, those conditions may change in the future. Additionally, if a customer approves his or her data to be collected and used for a particular purpose today, that does not mean the use could be different in the future. For example, although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (e.g., a conscientious exerciser is a good credit risk or will make a good employee).[30] Use of data for credit, insurance, and employment decisions could bring benefits—e.g., enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit—but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.[31]

The Fair Credit Reporting Act (FCRA) applies to third-party consumer reports used for credit or employment purposes; it requires consent for a report to be generated and allows that report to be reviewed for inaccuracies. The FCRA excludes most "first parties" that collect consumer information. Thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions—something that could become increasingly common as IoT develops.[32]

Consumers' tolerance of how companies use their data will depend on the company's transparency and how much trust the consumer has in the company with his or her data. Companies, marketers, and employers collecting data can de-identify data, but it is possible to re-identify data, especially if inadequate security measures are in place.

Demand Side of Wearables Market May Not Be Able to Address Data Privacy and Security

Targeted ads based on data gathered from wearables could reduce marketing spam for consumers and provide them with more relevant offers. Customer service can be improved and the gulf between offline and online shopping experiences can be bridged using wearable technology. Consumers, however, are increasingly more willing to view the data privacy and security of their personal data as more important than quality of service, and are starting to give false information for access to free services.[33] The trust consumers have in a company will influence how willing they are to reveal truthful personal information and how willing they are to have their data collected.

Nest Labs is a company known for its smart thermostat that can be controlled remotely by an app. The app learns a consumer's temperature preference and when he or she is home. The app does not collect much data about the consumer apart what it needs to function. Google acquired Nest Labs in January 2014 for over $3.2 billion in cash. Although Nest Labs has repeatedly insisted that it is not merging its data with Google's, consumers may not fully trust the company's assurances.[34]

Users are aware of the potential data privacy implications of wearables. One study specifically found that users are aware that when data are continuously collected, stored, published, and shared, they could include information that users would not want to recall later or would not be willing to capture or be reminded of later.[35] Users are also aware that when data from wearables are stored in the cloud, that data could be revealed without the user's knowledge or consent. Users' data privacy concerns primarily result from devices that include cameras and microphones followed by devices with GPS and displays. Activity trackers that monitor heart rate, steps, and pulse are seen by users as inoffensive to data privacy; however, the authors of the study postured that it is likely that users are not aware of how third parties

could misuse data or of the potential data privacy implications when the data are collected long term or associated with complementary information.

Conclusion

The technology supporting wearables began in a time when security risks were low and the end users were mainly businesses. Consumers have increasingly demanded technology over the past decades. Business models have changed requiring more and better consumer data. While wearables pose significant gains to consumers, especially in healthcare, a concerted effort must be made to address privacy and security. The current technological infrastructure supporting today's wearables have not addressed the security risks. The data privacy risks have not been addressed, and there are incentives for companies to gather more data than less from consumers. Consumers have shown that they are willing to trade privacy for lower cost, more innovative products. Where the demand or supply side of the market for wearables do not address privacy, policy or self-regulation should address the data privacy and security concerns posed by wearables.

Endnotes

1. *Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443.
2. Davey Alba, *50 Years On, Moore's Law Still Pushes Tech to Double Down*, WIRED (Apr. 19, 2015), http://www.wired.com/2015/04/50-years-moores-law-still-pushes-tech-double/.
3. Rob Stein, *Implantable Medical ID Approved by FDA*, WASH. POST, Oct. 14, 2004, http://www.washingtonpost.com/wp-dyn/articles/A29954-2004Oct13.html.
4. Robert McMillan, *It's Crazy What Can Be Hacked Thanks to Heartbleed*, WIRED (Apr. 28, 2014), http://www.wired.com/2014/04/heartbleed_embedded/.
5. FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 20 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
6. Sanjay Sarma, *I Helped Invent the Internet of Things. Here's Why I'm Worried about How Secure It Is*, POLITICO (June 2015), http://www.politico.com/agenda/story/2015/06/internet-of-thingsprivacy-risks-security-000096.

—. *Id.*

—. *Id.*

1. *See* Stanford Univ., TSensors Summit for Trillion Sensor Roadmap (Oct. 23–25, 2013), http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf [hereinafter TSensors Summit].
2. Carole Jacques, *Led by Samsung, Wearable Electronics Patents Are Growing at over 40% Annually*, LUX RES. (June 30, 2015), http://www.luxresearchinc.com/news-and-events/press-releases/read/led-samsung-wearable-electronics-patents-are-growing-over-40.
3. Anthony Mullen, *Fearing the Quantified Life—Privacy, Data and Wearable Devices*, THE NEXT WEB (June 5, 2015), http://thenextweb.com/insider/2015/06/05/fearing-the-quantified-life-privacydata-and-wearable-devices/.
4. Jeff Beer, *Your Heart Does the Swiping on This Hands-Free Tinder App for Apple Watch*, FAST COMPANY (July 6, 2015), http://www.fastcocreate.com/3048244/your-heart-does-the-swiping-on-thishands-free-tinder-app-for-apple-watch.

13. THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA 108–09 (2014).
14. Paul Krugman, *Apple and the Self-Surveillance State*, N.Y. TIMES, Apr. 10, 2015, http://krugman.blogs.nytimes.com/2015/04/10/apple-and-the-self-surveillance-state/?_r=4&assetType=opinion.
15. *Id.*
16. Allen P. Grunes & Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, 14 ANTITRUST SOURCE, no. 4, Apr. 2015, at 1, 2.

17. James Vincent, *Apple CEO Tim Cook: Unlike Other Companies, We Don't Want Your Data, Just Your Money*, INDEP. (Sept. 16, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/ apple-ceo-tim-cook-unlike-other-companies-we-dont-want-your-data-just-your-money-9735212.html.
18. Brad Brown et al., *Are You Ready for the Era of "Big Data"?*, MCKINSEY Q., Oct. 2011, http://www.mckinsey.com/insights/strategy/are_you_ready_for_the_era_of_big_data.
19. Mullen, *supra* note 11.
20. Id.

21. Comments of AT&T Inc. at 8, Workshop to Explore Privacy and Security Implications of the Internet of Things (F.T.C. May 31, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/ public_comments/2013/07/00004-86142.pdf.
22. See TSensors Summit, *supra* note 9.
23. FTC STAFF REPORT, *supra* note 5, at 7.
24. Id.
25. Krugman, *supra* note 14.
26. Jennifer Britton-Colonnese & Devin Steenkamp, *Continuous Blood Glucose Monitoring in Newly Diagnosed Type 1 Diabetes*, ENDOCRINOLOGY ADVISOR (Jan. 9, 2015), http://www.endocrinologyadvisor.com/diabetes/continuous-glucose-monitoring-in-type-1-diabetes/ article/391865/.
27. Comments of AT&T Inc., *supra* note 21, at 5.
28. TRAPX LABS, ANATOMY OF AN ATTACK: MEDICAL DEVICE HIJACK (MEDJACK) 5 (May 7, 2015).
29. Id. at 6.
30. FTC STAFF REPORT, *supra* note 5, at 16.
31. Id.
32. Id. at 17.

33. Nicole Kobie, *Tech Firms Need to Use Data Ethically around the Internet of Things*, GUARDIAN (June 10, 2015), http://www.theguardian.com/technology/2015/jun/10/tech-firms-need-use-dataethically-internet-of-things.
34. Allison Kade, *How to Manage the Threats to Our Privacy and Financial Security in the Digital Age*, THE STREET (June 17, 2015), http://www.thestreet.com/story/13188985/1/how-to-manage-thethreats-to-our-privacy-and-financial-security-in-the-digital-age.html.
35. Scott Amyx, *Data Privacy Playbook for Wearables and IoT*, INFORMATIONWEEK (June 8, 2015), http://www.informationweek.com/mobile/mobile-devices/data-privacy-playbook-for-wearables-and-iot/a/d-id/1320690.

Court of Justice of the European Union

PRESS RELEASE No 117/15

Luxembourg, 6 October 2015

Judgment in Case C-362/14

Maximillian Schrems v Data Protection Commissioner

The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid

Whilst the Court of Justice alone has jurisdiction to declare an EU act invalid, where a claim is lodged with the national supervisory authorities they may, even where the Commission has adopted a decision finding that a third country affords an adequate level of protection of personal data, examine whether the transfer of a person's data to the third country complies with the requirements of the EU legislation on the protection of that data and, in the same way as the person concerned, bring the matter before the national courts, in order that the national courts make a reference for a preliminary ruling for the purpose of examination of that decision's validity

The Data Protection Directive1 provides that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate level of protection of the data. The directive also provides that the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or its international commitments. Finally, the directive provides that each Member State is to designate one or more public authorities responsible for monitoring the application within its territory of the national provisions adopted on the basis of the directive ('national supervisory authorities').

Maximillian Schrems, an Austrian citizen, has been a Facebook user since 2008. As is the case with other subscribers residing in the EU, some or all of the data provided by Mr Schrems to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States, where it is processed. Mr Schrems lodged a complaint with the Irish supervisory authority (the Data Protection Commissioner), taking the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country. The Irish authority rejected the complaint, on the ground, in particular, that in a decision of 26 July 20002 the Commission considered that, under the 'safe harbour' scheme,3 the United States ensures an adequate level of protection of the personal data transferred (the Safe Harbour Decision).

The High Court of Ireland, before which the case has been brought, wishes to ascertain whether that Commission decision has the effect of preventing a national supervisory authority from investigating a complaint alleging that the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data.

In today's judgment, the Court of Justice holds that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the directive. The Court stresses in this regard the right, guaranteed by the Charter, to the protection of personal data and the task with which the national supervisory authorities are entrusted under the Charter.

The Court states, first of all, that no provision of the directive prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision. Thus, even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive. Nevertheless, the Court points out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid. Consequently, where a national authority or the person who has brought the matter before the national authority considers that a Commission decision is invalid, that authority or person must be able to bring proceedings before the national courts so that they may refer the case to the Court of Justice if they too have doubts as to the validity of the Commission decision. It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid.

The Court then investigates whether the Safe Harbour Decision is invalid. In this connection, the Court states that the Commission was required to find that the United States in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter. The Court observes that the Commission did not make such a finding, but merely examined the safe harbour scheme.

Without needing to establish whether that scheme ensures a level of protection essentially equivalent to that guaranteed within the EU, the Court observes that the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. The United States safe harbour scheme thus enables interference, by United States public authorities, with the fundamental rights of persons, and the Commission decision does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference.

The Court considers that that analysis of the scheme is borne out by two Commission communications,4 according to which the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the persons concerned had no

administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court finds that, under EU law, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. The Court adds that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.

Likewise, the Court observes that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law.

Finally, the Court finds that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Court holds that the Commission did not have competence to restrict the national supervisory authorities' powers in that way.

For all those reasons, the Court declares the Safe Harbour Decision invalid. This judgment has the consequence that the Irish supervisory authority is required to examine Mr Schrems' complaint with all due diligence and, at the conclusion of its investigation, is to decide whether, pursuant to the directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

2 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

3 The safe harbour scheme includes a series of principles concerning the protection of personal data to which United States undertakings may subscribe voluntarily.

4 Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, 27 November 2013) and Communication from the

Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final, 27 November 2013).

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.