

Wearable Technology: Key Legal Implications

Olivera Medenica
Medenica Law PLLC
3 Columbus Circle, 15th Fl.
New York, NY 10019
Tel: (212) 785-0070
Email: Omedenica@Medenicalaw.com

Legal Considerations with New Technology

Advertising
Claims

Multiple
Governmental
Agency
Regulations



Consumer
Product
Safety

Data Privacy
&
Cybersecurity

Sourcing,
Import and
Customs

Intellectual
Property

Industry Impact

- Top trends at the Consumer Electronics Show held in Las Vegas in January 2014.
- One of the buzzwords at February's Mobile World Congress in Barcelona.
- According to a 2015 Credit Suisse report, the market for wearable technology is currently worth between \$3 billion and \$5 billion, and it is expected to reach \$70 billion by 2050.
- The wearables market exceeded \$2 billion in 2015, and is expected to hit 4 billion in 2017.
- Just under 50 million wearable devices were shipped in 2015 and over 125 million units are expected to ship in 2019.

Industry Impact

- Growth in the wearables market is expected to increase 35% by 2019.
- Companies are beginning to test wearables in basic use cases like workplace security access (23%), employee time management (20%), and real time employee communication (20%).
- Employees equipped with wearable technology reported a 8.5% increase in productivity and a 3.5% increase in job satisfaction.
- Companies are also beginning to embrace “bring your own wearable” (BYOW) models with 54% currently supporting a BYOW model and an additional 40% planning to support this model in the future.
- Over 50 billion internet-connected devices will exist worldwide by 2020.
- 51% of people surveyed cited privacy as their biggest concern with wearable tech.
- One in six consumers currently owns and uses wearable tech.

Internet of Things (“IoT”)

- An interconnected environment where all manners of objects have a digital presence and the ability to communicate with other objects and people.
- Wearable computers, smart health trackers, connected smoke detectors and light bulbs.
- Any Internet connected device that is not a mobile phone, tablet, or traditional computer.

What is it?



Baby Sensors (e.g. Mimo)

A baby onesie equipped with sensors communicating to the mother the baby's temperature, heart rate and sleep patterns.



Smart Wristbands (e.g. SmartBand)

Smart Sensors on the back of watches and wristbands that track various physiological functions.

RINGLY



BLACK ONYX



EMERALD



PINK SAPPHIRE



RAINBOW
MOONSTONE

Smart Jewelry (e.g. Ringly)

Stylish rings that connect users to their phones and send notifications through vibrations and light.



Smart Clothing (e.g. Navigate Jacket)

Jackets that get the wearer from point A to point B by tapping on the wearer's back or flashing lights.



LED light dresses

Dresses equipped with thousands of LED lights that are controlled by an iPhone and can change colors and flash patterns.



Google Glass

OMsignal Biometric Smartwear

Smart Shirt. Smart App. Smart Results.



Heart Rate
Monitor



Calorie
Counter



Step
Counter



Breathing
Monitor



Fitness
Tracker

THE NEXT EVOLUTION
OF WEARABLE TECHNOLOGY

POLO

RALPH LAUREN

THE POLO TECH SHIRT

WE ARE PROUD TO BE THE FIRST LUXURY LIFESTYLE
BRAND TO OFFER APPAREL THAT TRACKS AND
STREAMS REAL-TIME BIOMETRIC DATA DIRECTLY TO
YOUR SMARTPHONE OR TABLET



POWERED BY 

CUFF

Limited Quantity

Pre-Order



Notifications with a buzz

Never miss a call or text again.



CuteCircuit



TWITTER DRESS

Attracting high-end market players Considerations with collaborations



Hermès & Apple



Opening
Ceremony & Intel

The continuous search for additional battery life



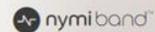
Rebecca Minkoff &
Case-Mate

Tommy Hilfiger &
Pvilion

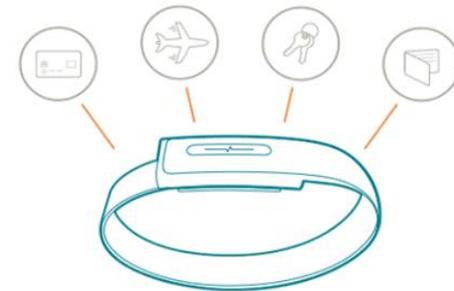


YOUR EVERYDAY SIMPLIFIED

Seamlessly unlock devices, remember passwords and more, using your heart's unique signature.

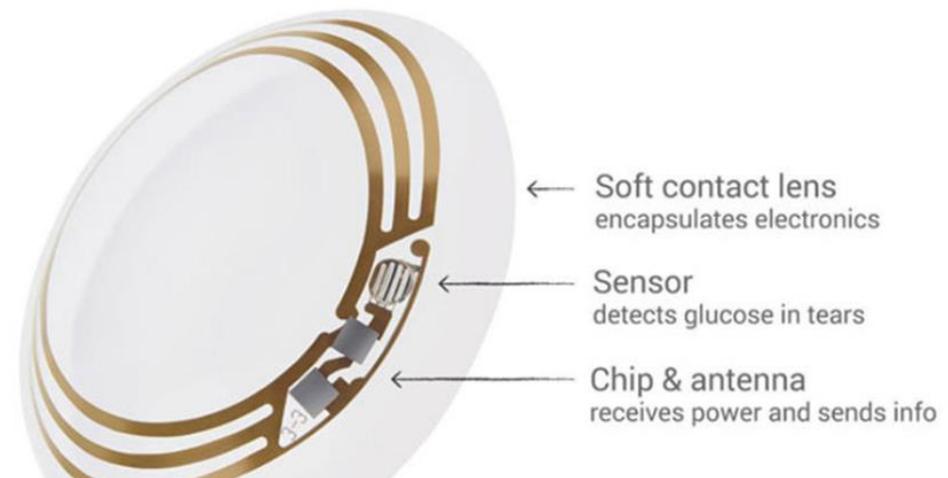
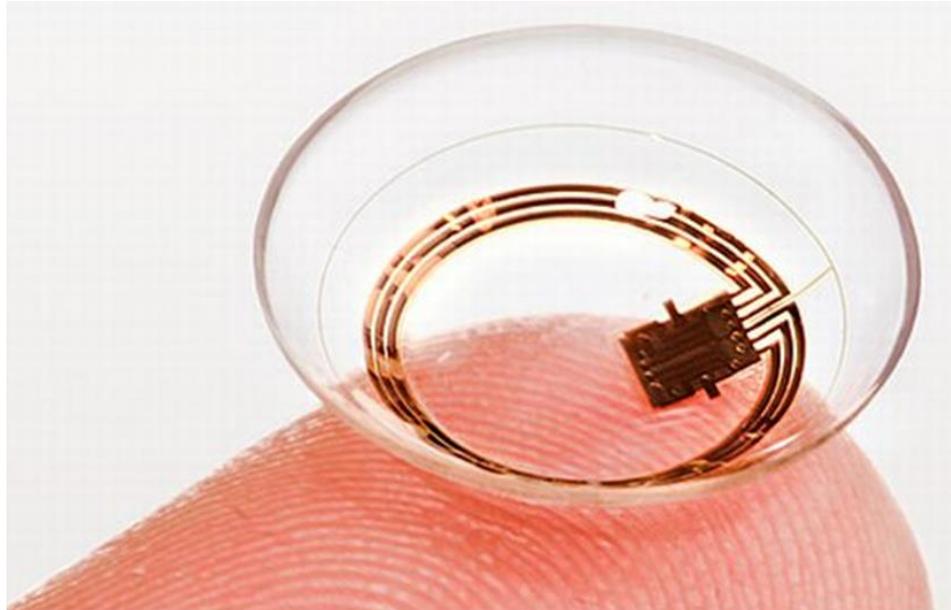
[RESERVE NOW](#)[WATCH VIDEO ▶](#)

Using HeartID, Nymi's patented biometric authentication technology, The Nymi Band is able to confirm your identity using your heart's unique signature.



The Nymi Band can then be paired with the devices and services of your choice, creating a world of seamless experiences.

Google



What are the benefits
of wearables?

Potential Benefits

- Health care: insulin and blood-pressure cuffs that connect to a mobile app; patients can give caregivers, relatives, and doctors access to their health data through apps; improved quality of life; disease prevention; tailored medications based upon constant data dialogue between patient and doctor.
- More efficient energy usage: smart meters can enable providers to analyze consumer energy usage.
- Home automation systems: single platform connecting all the devices within a home.
- Car and road safety: smart sensors on cars can alert driver of dangerous road conditions

What are the risks of wearables?

Security Risks

- Enabling unauthorized access and misuse of personal information;
- Facilitating attacks on other systems; and
- Creating safety risks.

Privacy Risks

- Collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information.
- Collection of personal information, habits, locations and physical conditions over time.

Privacy (con't)

- Volume of data: fewer than 10,000 households can generate 150 million discrete data points per day, approximately one datapoint every six seconds for each household.
- Sensitive data can provide beneficial services to consumers, but also increases the risk of unauthorized uses.
- Companies might use this data to make credit, insurance and employment decisions. Such use might be problematic without the consumers' knowledge or consent.

Privacy (con't)

- Consider the Fair Credit Reporting Act (“FCRA”)
- The 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 viewed for inaccuracies.
- The Act imposes certain limits on the use of consumer data to make determinations about credit, insurance, employment or related purposes.
- Imposes obligations on covered agencies, such as employing reasonable procedures to ensure maximum possible accuracy and access to gathered data.
- The Act, however, excludes “first parties.”

Privacy (con't)

- Creepy eavesdropping.
- Marketers want to know what you do at home, when you shut the door.
- IoT devices open the door to accessing this valuable information.

Significant Legal Issues

- Wearables raise a number of significant legal issues with respect to data obtained from the user and third parties.
- Vast majority of wearables currently focus on sensitive health-related and even biometric data.
- While the wearable captures and processes data collected from the user, the data is subsequently stored by the technology company.
- Adequate safeguards must be in place to protect this data.
- Safeguards must comply with the regulatory frameworks of both where the data is collected and where it is stored.

Traditional Privacy Principles

Fair Information Practice Principles (“FIPPs”)

- Notice
- Choice
- Access
- Accuracy
- Data minimization
- Security
- Accountability

FIPPs found in:

- Organization for Economic Cooperation and Development (“OECD”) privacy guidelines.
- European Union Directive on the protection of personal data.
- Health Insurance Portability and Accountability Act (“HIPAA”).
- Network Advertising Initiative Code of Conduct.
- Obama Administration’s Consumer Privacy Bill of Rights.
- FTC’s Report on Protecting Consumer Privacy in an Era of Rapid Change (2012).

Recent Developments

- May 2014, White House released a Big Data report.
- President's Council of Advisors on Science and Technology released a companion report.
- September 2014, Europe's Article 29 Working Group issued an Opinion on Recent Developments on the Internet of Things.
- August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices.
- January 2017, Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team issued an Internet of Things report entitled *Fostering the Advancement of the Internet of Things*.

HIPAA Basics

- The Health Information Portability and Accountability Act protects the privacy of an individual's health information.
- HIPAA's protections are enforced through the Privacy Rule – or federal regulations promulgated by the U.S. Department of Health and Human Services.
- Prohibition on “covered entity” from disclosing or unlawfully using a person's “individually identifiable health information” without specific written consent.
- Civil penalties range from \$100 to \$50,000 per violation.

EU Data Protection

- EU Data Protection Directive is expected to be replaced with the uniform General Data Protection Regulation (GDPR) in May of 2018.
- Expanded territorial reach: applies to data controllers and processors outside the EU whose processing activities relate to the offering of goods and services (even if for free) to, or monitoring the behavior (within the EU) of, EU data subjects.
- GDPR places onerous accountability obligations on data controllers to demonstrate compliance.
- GDPR establishes a tiered approach to penalties for breach which can result in fines for up to the higher of 4% of annual worldwide turnover or 20 million euros.

Privacy Best Practices

Data Security

- Security by design.
- Personnel practices must promote good security.
- Due diligence that service providers that can provide reasonable security.
- Defense-in-depth approach.
- Reasonable access control measures.
- Monitor & patch.

Data Minimization

- Reasons for data minimization.
- Reasonable expectations of consumers.
- Does the data relate to the product's direct purpose?
- Maintain it in de-identified form?
- Policies for not re-identifying the data.

Notice and Choice

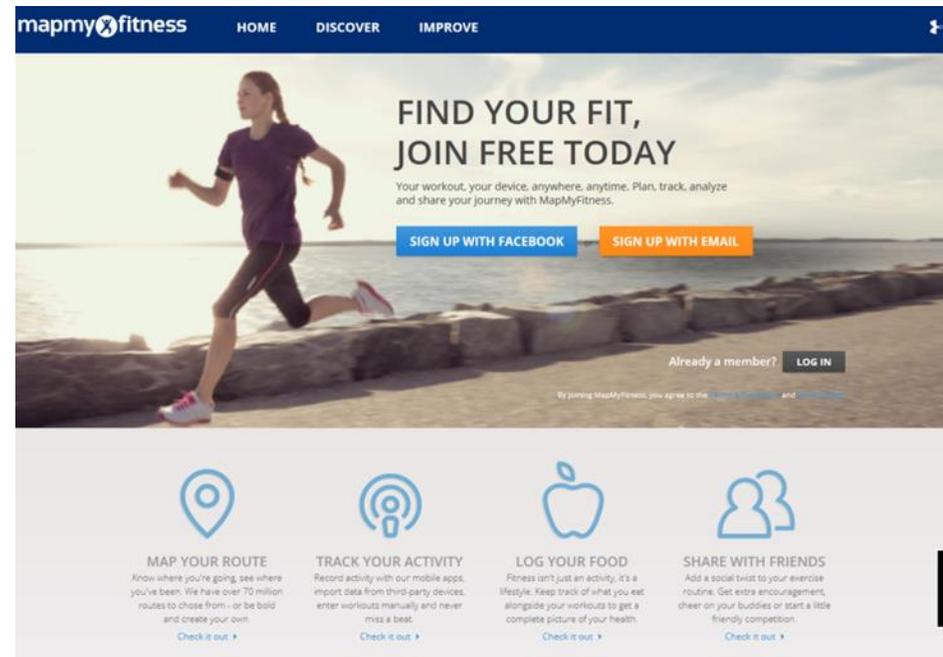
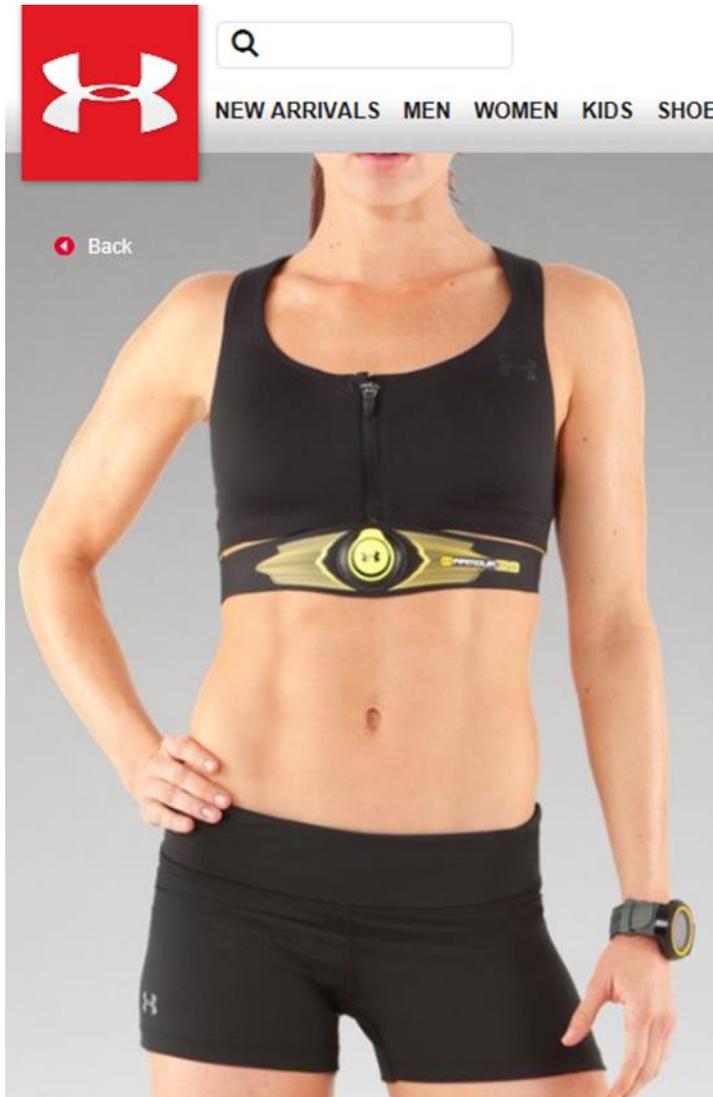
- Notice and choice not necessary when collecting/using consumer data for practices that are consistent with context of transaction.
- Choice at point of sale.
- Tutorials.
- Codes on device.
- Choices during set-up.
- Management portals and set-up.

Political Climate

- January 2015, FTC came out with a report entitled the “Internet of Things”
- One of the recommendations is that Congress consider enacting broad-based privacy legislation.
- Without legislation, FTC cannot mandate certain basic privacy protections, absent a specific showing of deception or unfairness.
- January 2017, DOC issues IoT report. One of the recommendations is to “[c]ontinue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness to cybersecurity, privacy, intellectual property, the free flow of information, digital inclusion, interoperability, and stability related to IoT.”

Notable Cases

adidas AG v. Under Armour, Inc. and MapMyFitness, Inc.



Valencell, Inc. v. Fitbit Inc. and Apple, Inc.

VALENCCELL



In the Matter of Genesis Toys and Nuance Communications



Intellectual Property/ Trademarks

Intellectual Property/TMs

- Product configuration
- Color
- Sound
- Motion marks
- Scent marks

Intellectual Property/Copyright

- Key issues: ownership, access and usage of data and software.
- Can the data be copyrighted?
- Copyright protection for the underlying software
- Design

Intellectual Property/Patents

- Technology
- Design

Intellectual Property/Trade Secrets

- Customer lists, methods of production, marketing strategies, pricing information, and chemical formulae.
- Algorithms
- “[p]roducts will be defined by the sophistication of their algorithms. Organizations will be valued based not just on their big data, but the algorithms that turn that data into actions and ultimately customer impact.”
- Defend Trade Secrets Act of 2016

Labor/Employment

Labor & Employment

- Lesson from the dual use devices.
- Legitimate business purpose v. Employee resentment.
- E.g.: detecting fatigue in medical professionals; monitoring a production line for quality control purposes.
- Companies should establish a policy addressing the business purpose of the data collected from employees wearing the wearable device.
- Limits should be placed on the gathering of personal and private information about employees.
- Actions implemented to secure this information.
- Company wide policies and training.

EEOC New Rule on Employer Wellness Programs

- Amends the regulations under Title I of the Americans with Disabilities Act and the regulations under Title II of the Genetic Information Nondiscrimination Act as they relate to employer wellness programs.
- “wellness program” refers to health promotion and diseases prevention programs and activities offered to employees.
- Title I of the ADA generally restricts employers from obtaining medical information from applicants and employees but allows employers to make inquiries about employee health programs which includes many wellness programs.
- “reasonably designed to promote health or prevent disease”
- Must be voluntary
- Medical records developed in the course of providing wellness programs must be maintained in a confidential manner.

Product Liability

Fitbit Recalls Force Activity-Tracking Wristband Due to Risk of Skin Irritation

Consumers should stop using this product unless otherwise instructed. It is illegal to resell or attempt to resell a recalled consumer product.

Recall date: MARCH 12, 2014

Recall number: 14-129



Recall Summary

Name of product:

Wireless activity-tracking wristband

Hazard:

Users can develop allergic reactions to the stainless steel casing, materials used in the strap, or adhesives used to assemble the product, resulting in redness, rashes or blistering where the skin has been in contact with the tracker.

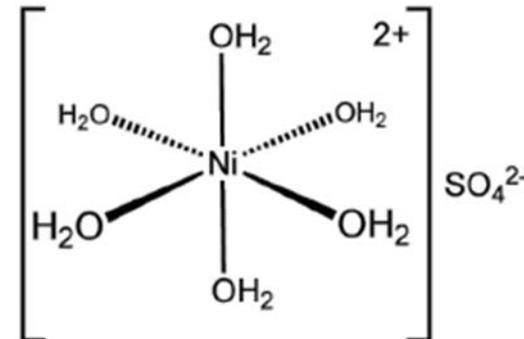
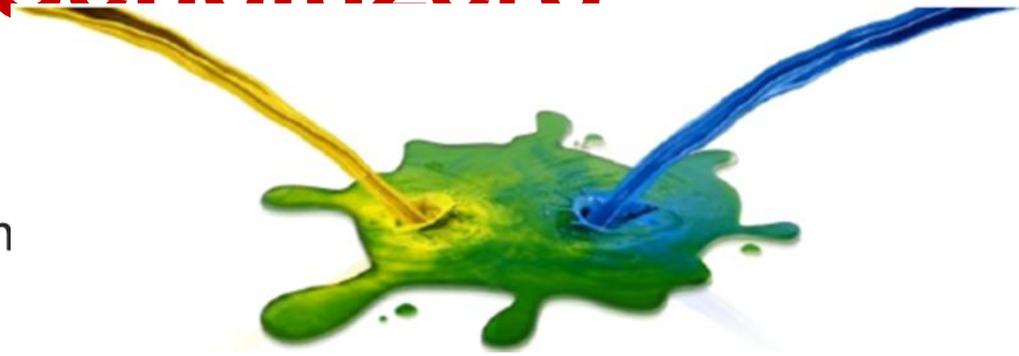
Remedy:

[View Details](#)

Refund

Skin Allergens/Sensitizers

- Additives
 - PPD or p-Penylenedian
 - Cobalt
 - Glyceryl thioglycolate
- Metals
 - Nickel
- Elastic Materials
- Latex
- Leather
 - Chromium
 - Glutaraldehyde

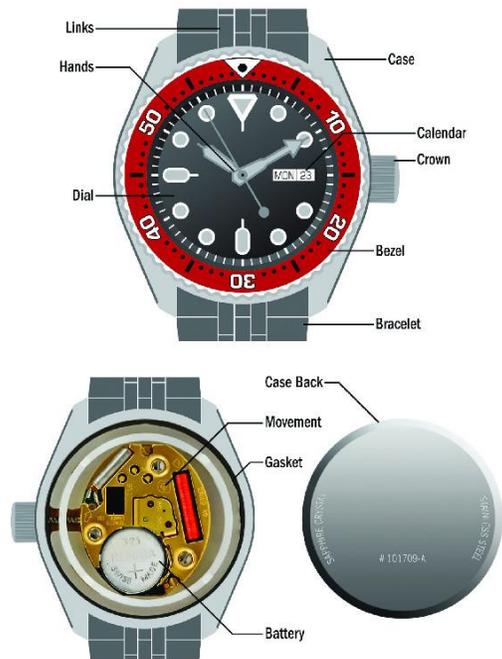


Importing Considerations

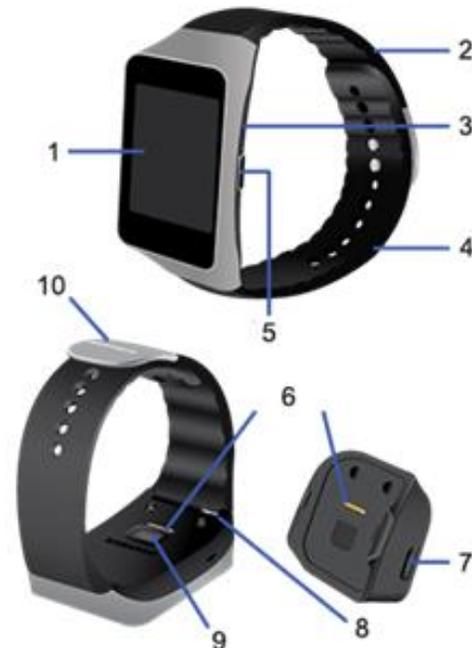
Selling & importing wearables

- Example:
- Smart watch ([CBP Ruling HQ H257947](#) July 14, 2015)
 - Issue: How is a smart watch classified under the tariff code regime?

Components of a traditional watch



Components of a smart watch



1. Screen; 2. Upper strap; 3. Microphone; 4. Lower strap; 5. Power button; 6. Charging terminals; 7. USB port; 8. Strap release; 9. Heart Rate sensor; 10. Clasp.

HTSUS analytical framework

- Classification according to General Rules of Interpretation (GRI)
 - GRI1 Classification determined according to the “**terms of the headings of the tariff schedule and any relative Section or Chapter Notes.**”
 - GRI3 ... if an item is **classifiable in two or more headings**, classification shall be determined by effected as follows:
 - (a) ... the heading which provides the **most specific description** shall be preferred...
 - (b) Mixtures, composite goods consisting of different materials or made up of different components, and goods put up in sets for retail sale, which cannot be classified by reference to 3(a), shall be classified as if they consisted of the material or component which gives them their **essential character**, insofar as this criterion is applicable.

What is “it”?

HTS Headings considered by CBP in HQ H257947:

- **8517** Telephone sets, including telephones for cellular networks or for other wireless networks; other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network (such as a local or wide area network), other than transmission or reception apparatus of heading 8443, 8525, 8527 or 8528; parts thereof:
- **8519** Sound recording or reproducing apparatus:
- **8521** Video recording or reproducing apparatus, whether or not incorporating a video tuner:
- **9029** Revolution counters, production counters, taximeters, odometers, pedometers and the like; speedometers and tachometers, other than those of heading 9014 or 9015;
- **9031** Measuring or checking instruments, appliances and machines, not specified or included elsewhere in this chapter; profile projectors; parts and accessories thereof:
- **9102** Wrist watches, pocket watches and other watches, including stop watches...

An uncomfortable fit

- Smart watches do not share any characteristics with traditional watches except case, strap and other cosmetic features
 - Key features of the watch is not telling time, but to send & receive messages (email, texts, notifications), run apps, play music, collect data (fitness, steps, heart rate), connect to wireless
 - Smart watches require FCC certifications to be sold in the US
- Watches HTS Heading 9102 = dutiable (typically per watch rate + separate *ad valorem* rates on case + strap, band or bracelet + battery)
- Smart watches HTS Heading 8517 = Free

Wearables - what's next?

- Move from watches and bracelets to more innovative categories such as clothes and independent devices (no pairing required)
 - Examples:
 - Project Jacquard (Google smart tag & Levi's®)
- From an import perspective, will the tariff schedule catch up?
 - Apparel historically subject to significant duties
 - Electronics are generally free or low duty
- Globally, customs authorities everywhere are grappling with these hybrid products but most are slow to catch up...

E-Discovery

New Frontier in Discovery Disputes

- Can track every part of the user's day, including activity, exercise, food, weight and sleep.
- Virtual "black box" for the human body.
- Informal discovery may be a viable option where the user's profile is public.
- If profile is private, then more formal discovery efforts are necessary.
- Ownership of data: user or social networking site?
- Time is of the essence: spoliation issues and litigation hold letters.

The End...

Olivera Medenica
Medenica Law PLLC
3 Columbus Circle, 15th Fl.
New York, NY 10019
Tel: (212) 785-0070
Email: Omedenica@Medenicalaw.com