The Federal Trade Commission's (FTC) staff report on the Internet of Things (IoT), culminating a year and a half of investigations, was recently released. Succinctly, the Internet of Things promises to connect 50 billion individual devices by the end of the decade. With many of these devices sensing, tracking, and reporting on your personal and private data to corporations, health care workers, and who knows who else, the growing pervasiveness of the IoT raises, among other concerns, non-trivial privacy, pan-device-compatibility and security issues that need to be dealt with to maintain the viability and commercial success of this emerging technology trend.

The FTC aimed to suggest a response to this deluge of information in its report. The report outlined how IoT products should be developed with security and minimal data collection and retention in mind. Additionally, the FTC suggested that consumers be provided notice of their data collection, and choices regarding the nature of that collection. While some would argue that this narrowly focused top-down regulatory approach will eventually chill innovation, we think there needs to be a middle ground between wholly unregulated permissionless innovation —ostensibly intended to promote out-of-the-box thinking and further innovation— argued for by some detractors, and the FTC's relatively overbearing alternative.

WHERE IS CONTRAST

DOV 1/4/16 2:06 PM
Deleted: , i.e., Bi,,,,,,,,cutg Data,

DOV 1/7/16 12:56 PM
Deleted: ,,,,,why bad,,,,.

DOV 1/7/16 12:56 PM
Deleted: t the proposal's

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

DOV 1/7/16 4:35 PM
Formatted: Font:Bold

We argue for a middle ground: And in particular, at least in some types of IoT devices, especially those related to healthcare, there ought to be specific oversight.

The necessity of this oversight will become all the more relevant with the development of the President's Precision Medicine Initiative, wherein personalized health data, many collected via pervasive IoT devices, will be amassed into databases to be analyzed and eventually even support health care decisions. Here, we are likely to see an even greater integration of the IoT and its devices within healthcare services. This integration, potentially across all IoT platforms that collect health-related information, will necessitate privacy protections and an unprecedented level of technical standardization, hence the need for oversight and some regulatory control.

DOV 1/7/16 12:58 PM
Deleted: will be

DOV 1/7/16 12:57 PM
Deleted: incorporated into an increasing number of health care decisions,,,,mention data sets,,,,.

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

The necessity of oversight is not limited to consumer protection, many in the basic science and medical research fields see this data as a godsend, enabling heretofore unachievable research opportunities. Clinical medicine also appreciates the potential value of this data, particularly in the management of chronic disease through the widespread use of mobile medical applications. Further, pharmaceutical companies are particularly keen on obtaining access to collected Big Data to support their personalized medicine research aimed at filling their drying drug pipelines. To wit, the US Food and Drug Administration (FDA) recently provided some guidelines for the use of Mobile Medical Applications (MMAs) for the software industry looking to sell apps to monitor the large percentage of the population with chronic diseases; and, the United States government has only just announced, as part of the Precision Medicine Initiative, a two hundred million dollar initiative to bank one million user health profiles.

TOO CYNICAL

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 12:59 PM
Deleted: bio

DOV 1/7/16 12:59 PM
Deleted: .   ,,,,,not sure bio bank is right here?

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

The use of this sensor derived data in health care is no long science fiction. For example, Stanford's chair in Genetics, Professor Michael Snyder has developed a working system wherein millions of datapoints are collected, some through scientific experiments and others through wearables, to develop an integrative personal omics profile (iPOP). In a proof of concept, Professor Snyder created an iPOP of himself; the merging of all this data revealed heretofore unknown medical concerns.

The healthcare industries are not the only ones that will benefit from oversight that could include standardization across all platforms: UnderArmor, a global sports clothing and accessories company, recently purchased millions of consumer physical fitness profiles including billions of data points generated by the growing industry of fitness related wearables. Additionally, their UA Healthbox wearable products are designed to help consumers manage both fitness and health. The fitness industry is one of many consumer-facing industries that are aiming to exploit the emergent quantified-self trend wherein users use IoT technologies to keep track of, among other things, their fitness goals.

TOO NEGATIVE

Returning to privacy concerns, a growing cadre of powerful algorithms are ever-more capable of de-anonymizing even seemingly insignificant bits of this consumer fitness data and intruding further on consumer privacy. And those are just the legitimate stakeholders, others are intent on accessing and/or hijacking your data, be it at rest, in use, or in motion.

SOUNDS LIKE GOSSIP USE REF

While encryption and other security efforts might potentially help protect consumer privacy as their wearables, smartphones, health related devices and other components of the IoT beam data back to any number of masters, companies are reportedly loathe to incorporate computationally heavy and battery-hogging encryption, and users tend not to enable such encryption even when the option is available. Moreover, any solution could be further complicated by uncooperative or antagonistic governments set on being able to intercept encrypted terrorist communications, as evidenced by the United Kingdom recent but failed efforts to ban WhatsApp, SnapChat, and other end-to-end encrypted communications

Any solution to these global problems will be non-trivial and will necessarily require technological, regulatory and social change. However, barring international cooperation at the government level, it is unlikely that legal or legislative solutions will be found any time soon. Perhaps de facto legislating through technology will provide a more immediate solution; as such, technological developments are necessary to promote interoperability among the devices and better use of the data once it is collected from multiple sources.

Interoperability is far from trivial. Each of these devices contains a number of sensors, measuring physical quantities for conversion into computer readable signals. These sensors include, for example those that measure motion, orientation and environmental conditions. Each device could potentially have a distinct set of sensors and each of these sensors may interact differently (albeit sometimes minimally so) with the wide variety of operating systems and their respective versions. Outside variables can also affect the sensors, for example, even prolonged exposure to refrigerator magnets can decalibrate

DOV 1/7/16 1:00 PM
Deleted: Although Snyder's efforts focused on molecular data, the methods could easily be expanded to include vitals data collected from wearables and/or smartphone sensors. ,,,,he's using wearables now

DOV 1/7/16 4:35 PM
Formatted: Font color: Red

DOV 1/7/16 4:35 PM
Formatted: Font color: Red, Not Highlight

DOV 1/7/16 4:42 PM
Deleted: s.

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 1:01 PM
Deleted: ,,,,,,need refs

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto, Not Highlight

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 1:01 PM
Deleted: . In addition,

DOV 1/7/16 1:01 PM
Deleted: governments on shaky legal grounds and shadowy criminal enterprises

DOV 1/7/16 1:01 PM
Deleted: ,,,,para is too strong. ....,,,,,,,,

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto, Not Highlight

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 1:02 PM
Deleted: And

DOV 1/7/16 1:02 PM
Deleted: treaties and

DOV 1/7/16 1:02 PM
Deleted: n,

DOV 1/7/16 1:02 PM
Deleted: can

DOV 1/7/16 1:02 PM
Deleted: .

DOV 1/7/16 1:03 PM
Deleted: ,,,,,non sequitur

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto, Not Highlight

DOV 1/7/16 4:35 PM
Formatted: Font color: Auto

DOV 1/7/16 1:03 PM
Deleted: A

some magnetometers. REF Data among different sensors, particularly those developed primarily for recreational use is often inconsistent and can vary widely across platforms and even among body characteristics.[1]

DOV 1/7/16 4:53 PM
Formatted: English (US)

In addition to the necessity of standardization to prevent different sensors from providing uncalibrated readings, standardization will also be necessary to promote data consistency, for example, such that readings are all provided using the same formulas and the same units to allow for comparisons across wearable platforms. The IoT especially suffers from the lack of standardized data formatting and standardized encryption, perhaps because at least 5 distinct organizations are vying for the position as the standard setting body of the IoT. REF This makes it harder to collect, decrypt and analyze the data, and keep that private data safe and secure.

DOV 1/7/16 1:52 PM
Deleted: .

Further, the usability of this data for large-scale research efforts is hampered by the lack of consistency among devices making up the IoT. For example, there are hundreds of millions of smartphones and wearable devices in the world with a myriad number of distinct and diverse models running a variety of operating systems and their respective versions. Additionally, there is a multitude of application on these devices that might further alter basic operating aspects, (and as a result their sensors as well) of the phone either unintentionally or even maliciously.

HARDER FOR ANALOG V DIGITAL

Given all this variability it would seem nearly impossible to consistently and safely collect reliable, accurate and/or medically actionable data, questioning the feasibility of this paper's premise: that the IoT can be useful in the area of healthcare and academic research.

+ ITS HIGHLY STANDARDIZED PLATFORM

Arguably Apple has attempted to work around these issues with its proprietary health collecting software and closed environment: HealthKit. Apple has seemingly already benefited from this standardization through collaborations with multinationals that appreciate the standardization and reliability of Apple's data. However, in creating a system that relies on users to trust a single large wealthy company with all the health related sensor data, standardizing it, and ensuring our privacy is perhaps not a good idea. In fact, research suggests that companies are not trusted with health related data;[2] many consumers and practitioners might prefer that a trusted, cross-platform, non-conflicted third party be the intermediary.

DOV 1/7/16 1:53 PM
Deleted: . ,,,H

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

DOV 1/7/16 1:53 PM
Deleted:

DOV 1/7/16 4:35 PM
Formatted: English (US)

Apple's solution uses, although not necessarily requires, middleware that works closely with the phone. To some degree the closer the standardization process is to the phone, the less the raw data needs to travel from their source and the less likely it will be hijacked in transit. However, requiring the middleware to work on the phone requires the necessary computing power to calibrate the sensors, analyze and standardize the data as well as encrypt it for further travel.

DOV 1/7/16 4:51 PM
Formatted: Space After: 0 pt

DOV 1/7/16 4:35 PM
Formatted: English (US)

[1] http://www.technologyreview.com/review/538416/the-struggle-for-accurate-measurements-on-your-wrist/

[2] http://www.technologyreview.com/news/543536/tech-companies-are-not-trusted-with-health-data/

GENERALIZING...
BASED ON THE APPLE EXP....

OPEN SOURCE

For all other platforms, including the most popular, Android, abstractly, a workable solution might include a middle-layer i.e., a shared interface for the exchange of information between the sensors and an end-point for the data. We could imagine that this unobtrusive middle-layer could be situated locally at the sensor or device that receives and reports the sensor's reading, such as a smartphone. This middle-layer could also be configured to encourage data integration and device interoperation, by requiring all data passing through the layer to be in a standardized format, and importantly, through regular updates, calibrate and statistically normalize the sensor outputs. This middle-layer would be tasked with promoting standardization of data encryption.

In the end, any solution should both promote innovation while at the same time protect the consumer by providing just-enough-industry-tailored oversight.

DID THIS HAPPEN OR WAS IT PROPOSED?

Some jurisdictions might achieve these goals via mandated top-down legislative solutions. Like the enforcement of V-Chip implementation in the 1990's that required every television set in the United States, Canada and Brazil to include a hardware component designed to protect children from questionable content, a similar hardware and/or software or hybrid solution could be mandated by government edict, or internal industry regulations, to be included in every data collecting device in the IoT. This middle-layer, the product perhaps of government, an NGO or a multi-national standard setting organization, could conceivably enforce, among other things, standardized encryption and other security arrangements for every device. While international organizations do exist to police some aspects of internet standardization, such as ICANN (domain naming conventions) and W3c (internet protocol standards) and other not-for profit public benefit organizations, it is unlikely that one of these organizations could enforce standardization in the IoT as well.

DOV 1/6/16 2:29 PM
Deleted: $$$,,,,prob w appl, see new text I'm sending!

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

DOV 1/7/16 4:35 PM
Deleted: ,,,,doesn't this exist

DOV 1/7/16 4:35 PM
Formatted: Not Highlight

DOV 1/7/16 4:35 PM
Deleted:

DOV 1/7/16 4:35 PM
Formatted: English (US)

Alternatively, a middle-layer could be an offsite clearing house. For example, a centralized third-party cloud site, configured to be the portal through which all consumer data would voluntarily pass. Like credit reporting agencies, these clearing houses, through directing all of your data through a single portal, could help consumers keep track of the overwhelming amount of data that they are generating and exporting and warn you of any malicious hijacking of that data.

The middle-layer site could be configured to only accept data that was provided in a standardized format, encrypted and the result of calibrated sensors. Consumer services could advertise, as a selling-point, that their data meets these standards and that it is passed through this third-party site. Like the options described above, this site could be run by a government, NGO, or private corporation, and funding could come from the IoT companies that use the site.

Blockchain technology could also be incorporated into process, particularly where it is important that verified data passes through to the intended recipient, such as in the case of health data reporting for chronic disease. Here, either the blockchain would provide independent verification as to the veracity of the data.

In the end, any solution should both promote innovation while at the same time protect the consumer by providing just-enough-industry-tailored oversight. The task we've outlined is by no means simple and would require extensive cooperation from all stakeholders. However it is necessary in order to usefully mine the onslaught of IoT data.