Introduction

The administration has proposed eight high level goals for federal action with the collection, retention and use of personal data of users. The eight goals are: (1) Harmonize the regulatory landscape, (2) Legal clarity while maintaining flexibility to innovate, (3) Comprehensive Application, **(**4) Employ a risk and outcome-based approach, (5) Interoperability, (6) Incentivize Privacy Research, (7) FTC enforcement, and (8) Scalability.

These comments will focus on Harmonizing the regulatory landscape. They will begin with an examination of global and United States regulations present or coming into fruition, with regards to the collection, retention, and use of personal data of users. These legislations will be compared, contrasted and analyzed, to show the issues that harmonization poses. In lieu of this, privacy legislation for the collection, retention and use of personal data of users should be focused around the protection of users. To implement a system where the user is at the forefront, Privacy must be recognized as a trust, and regulation must be placed to force privacy by design.

To begin, there are few sectoral laws that will be briefly explained. Then California Privacy Act, and Biometric Information Privacy Act will briefly be explained:

Federal Acts:

Gramm-Leach-Bliley Act[1] applies to financial institutions, and their method of handling nonpublic data in the United States. This act limits financial institutions from disclosing "nonpublic information" about consumers unless they follow three steps: a. they must provide their consumer a clear notice, b. they must give time for consumer to take a course of action before the information is disclosed, and c. they must give an option and explanation on how the consumer can opt out of this. (notice of choice model). The notice must clearly disclose the details of data and specify the third parties that the data is being given to. This act excludes public information about the consumer and has numerous exceptions (such as information necessary to administer a transaction will be excluded). Furthermore, financial institutions are barred from giving out sensitive information such as credit card numbers to nonaffiliated third parties (that they do not have a common ownership or control with) for marketing purposes.

The Health Insurance Portability and Accountability Act[2]: applies to health care providers, health plans, and "health care clearinghouses" which transmit any protected health information. It also applies to business associates in limited ways. This act prevents these providers, plans, and houses from disclosing/using an individual's protected health information (individually identifiable health information), without authorization from the individual, unless an exception applies. Some exceptions: they must disclose this information if the individual requests it, and they can use this information without authorization for treatment, relying on their best professional judgements. This act also limits use of the data to the "minimum necessary to accomplish their intended purpose".

[1] https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (for full pdf)
[2] https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (full pdf, see privacy rule)

Fair Credit Reporting Act[3]: regulates consumer rating agencies in the collection, use, and privacy of consumer information. This act sets strict parameters on how and when they can disclose consumer credit reports. One parameter is if employers seek an employee's credit report, the employee must give a written consent to the employer to do so. Another parameter is that agencies must disclose all information on files about the consumer if the consumer asks for it and have a right to know what is on file. (page 45,46). Lastly, agencies can only provide this information to people with a valid need (through an application). They also must delete any unverifiable inaccurate information.

State Legislations:

Biometric Information Privacy Act[4] (Illinois): is an Illinois State act that regulates the collection, storage, and disclosure of a person's biometric identifier/information. This Act states that an entity may not collect, store, disclose, sell, lease, or trade a person's biometric information without one of the following: (1) authorized consent, (2) if it is used to complete a financial transaction authorized by the persons identifier, (3) disclosure is required by state law, or (4) disclosure is required by a subpoena through a warrant. BIPA defines Biometric information as "a retina, or iris scan, fingerprint, voiceprint, or scan of hand or face geometry of a person.

California Privacy Act[5]: is the most expansive and detailed regulation of data collection, use, processing and disclosure in the United States. It entails an extensive list on what personal data is regulated. This act gives citizens of California, the right to request for all information that a business collects about them, requires businesses to inform consumers of what information before they collect them, and gives consumers the right to delete any information that businesses have about them

Analysis:

To harmonize is to find a common standard, or to "adjust differences and inconsistencies to make them uniform or mutually compatible."[6] The following will explain some core issues that arise when seeking harmony:

Conflict in Goals: Examining the federal and state privacy acts, the first issue with harmony is that Sectoral and State laws have different goals. The Sectoral laws regulate the "data collector" (financial institutions, health care providers, to consumer rating agencies). Biometric Information Privacy Act regulates the subject of the data. (regulating/barring the collection of biometric information). While the California Privacy Act is primarily concerned with user's privacy rights. An application of these legislative focuses can further construct this study. A smart watch provider has an inbuilt pre-installed application that passively collects, processes, and stores information about a user's location, heart rate, and total steps walked every day. This

[3] See https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf
[4] See http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57, for full text.

[5] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[6] http://www.businessdictionary.com/definition/harmonization.html

information is linked to the user's profile, with user input on the application. The sectoral approach would regulate the "technology sector", or "smartwatch industry" itself, setting disclosure and consent for the data being collected. The subject of the data approach is regulating the specific "passively tracked health care information" that the smart watch is collecting, processing, and storing. The California Privacy Act would be concerned with protecting the user's rights that use the smart watches. The California Privacy Act would seek to put the user's privacy at the forefront. While sectoral laws would allow the collection, processing, and use of data so long as there is a consent given, or written authorization given (HIPAA). This is conflicting.

Variance in the definitions of Personally Identifiable Data: Another inconsistency stems from defining personally identifiable data. Each of the federal acts imposes different constraints on how these types of data should be connected to the individual. HIPPA uses the term individually identifiable health information and defines it as information about the past, present or future mental or physical health an individual which identifies the individual, or reasonable basis to believe the information can be used to identify that individual. Gramm-Leach-Bliley Act: uses the term "non-public information" and limits this scope to any personally identifiable information which is provided by a consumer to a financial institution, from a transaction or otherwise obtained by the financial institution. This act differentiates "nonpublic" information from public information. Nonpublic information consists of financial data such as credit card numbers that derive directly from the transaction. Fair Credit Reporting Act defines consumer reports as: "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: a) credit or insurance, (b) employment purposes, or (c) any other purpose authorized under section 604. "

All four legislations emphasize that the data that should be protected should have a connection to the person of whom the data pertains to, but all four have different stringencies. HIPPA seeks to protect user's health information of any time... and there must merely be a reasonable belief that it could identify the individual. GLB limits the identifiable information to nonpublic information given to a financial institution from a financial transaction or other means. Fair Credit Reporting Act: seeks to protect any credit related information about the individual, Biometric Information Privacy Act: strictly applies to biometric data, and California Privacy Act has a very long and extensive list of what it considers as personal information.[7] This is confusing

[7] California Privacy Act defines Personal information as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or

as there is no clear-cut definition of what personal data or personally identifiable data is. It varies from sector to sector, and from different types of data. Thus, very difficult to find a clear definition.

Notice of Choice Models: Finally, every single legislation present explained above are based around a notice of choice model. The entities covered under the sectoral regulation are required to tell the user the information that is collected, the purpose, and to whom it is disclosed to and the user has an option to opt out or to deny this service. If the user opts out of the collection, processing, or use, then they cannot use the service. Thus, this creates an illusion that users have a choice. They really do not have any choice in any sectoral legislation. If they "opt out" then they have no access to the products they seek to use. So, the user has no choice but to accept that their personal data may be used, processed, disclosed or collected.

The European Model

Unlike the United States, EU has a comprehensive legislation (GDPR) and EU recognize privacy as a fundamental right. Article 8 of The EU Charter of Human Rights (used by the Court of Justice of the European Union (CJEU) states:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority."[8]

EU places the greatest priority on the protections of users for data regulations. Federal Action in the United States should follow this model, and place user protections over providing ease and flexibility for corporate entities, as they are the most vulnerable to harm.

Privacy by Trust & Privacy by Design

One approach that the FTC can take in protect citizens is recognizing that "privacy is a trust-based relationship". When people go to consult a lawyer or an accountant, they enter a fiduciary relationship. They have absolute trust, have absolute dependency, have absolute reliance on their expertise and are vulnerable their expertise. Ari Ezra Waldman in *Privacy as Trust* states that users enter the same expectations when using "information fiduciaries" such as Facebook as they do with doctors and accountants. Users depend on Facebook to engage in social interactions through their service. Users are vulnerable to Facebook's algorithm. User's trust Facebook companies in the safe keepings of their data, and Users rely on Facebook and other information fiduciaries marketed as "social connectors".[9] High-Level Goals for Federal

---

employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

[8] http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data

[9] See Page 85-87 of Privacy as Trust, Information Privacy for an Information Age by Ari Ezra Waldman.

actions should create a rigid set of regulations on corporate entities that user's trust. Rigid guidelines and punishments like the GDPR that would force strict liability to corporate entities that violate the regulations.

Second, High Level Goals for Federal Action should seek to mandate privacy by design, as it would be congruent with the goal of employing a risk and outcome-based approach. Privacy experts Woodrow Hartzog, Dr. Ann Cavoukian, and many others emphasize the value that this brings to privacy regulation. Privacy by design is the theory that privacy protections should be incorporated into the core functionalities of IT based systems. Requiring privacy measures as engineers from the start of a production of a product would push towards creating privacy as an essential component of its functionality.