**Hashed & Salted | A Privacy and Data Security Update**
December 2023

# A How-To Manual Determining Compatible Purposes for Connected Device Data

## To Be Compatible or Not To Be Compatible: That Is the Question

Wearable fitness trackers, smart TVs and connected cars are a few of the most commonly used consumer products that collect data and transmit that data to the device manufacturer, other device manufacturers, and consumers with similar devices. These devices are often referred to as the "Internet of Things" and "connected devices." Companies offering connected devices use the data from these devices to offer an array of convenient and sophisticated services to their customers. These services are typically the "primary purpose" disclosed in the marketing materials and privacy policy but may not be the only purposes disclosed. The data collected by these devices is typically deemed protected because it is tied to an individual consumer and is customarily considered "personal information" under data protection laws. For simplicity, we refer to personal information as "data" throughout.

Consumers who buy these connected products typically like to know how many steps they take in a day or their sleep pattern. They appreciate a curated personalized menu of programming on their TV. With one click of an app, these consumers happily warm up their connected cars from the comfort of their homes on a cold winter morning and expect to be able to locate their connected car in a crowded public parking lot via their app, using precise geolocation. Connected devices allow us to better connect to ourselves, interact with other people, and collect and exchange data across devices.

What's the trade-off? Connected devices require enormous amounts of data, which is typically accessed and used by the companies from which consumers purchase their connected devices. Companies have largely had free rein to use the data as they see fit (at least in the U.S.). Today, though, with the more extensive and continually evolving data protection legal landscape, businesses must engage in a complex analysis around utilization of that data.

This how-to manual explains what connected devices can do and the types of data they can collect, describes the purpose limitation on uses of data beyond the primary purpose," (i.e., the compatibility question), how to answer that compatibility question, and a use case to bring it all together.

*Attorney Advertising*

## Where to Begin?

Consider the following Internet of Things, the types of data these devices typically collect, and how the devices can be interconnected:

1. Smart thermostats measure and track the temperature and humidity levels inside and outside the home and collect user preferences and patterns of heating and cooling usage.
2. Wearable fitness trackers collect heart rates, step counts, sleep patterns, calories burned, and sometimes location data.
3. Smart refrigerators collect internal temperature, usage patterns, and inventory of items stored.
4. Connected cars track vehicle speed, location, fuel consumption, engine health, and driver behavior.
5. Smart TVs collect viewing habits, content preferences, and sometimes ambient noise or voice commands.
6. Health monitoring devices collect vital signs (blood pressure, heart rate), blood glucose levels, and medication adherence.

As businesses recognize they are sitting on a treasure trove of data, it is hard not to consider all of the possible uses for that data. The Fair Information Privacy Principles (FIPPs), data protection laws, and regulators around the world have attempted to reign in these additional uses by requiring purpose limitation data minimization. "Purpose limitation" is a legal phrase that intends to restrict how a business uses data collected from a consumer. Likewise, data minimization is a legal phrase that intends to restrict how much data a business can collect in the first place. Data minimization is not the focus of this manual but is a factor in determining compatibility.

## What Makes a Particular Use of Connected Device Data Compatible or Incompatible?

To start, businesses need to ask themselves whether "other" disclosed use cases are compatible enough with the primary purpose. Making this determination is difficult given limited regulatory guidance, which (unsurprisingly) varies from jurisdiction to jurisdiction.

That said, the practice of "purpose limitation" follows two general principles:

1. Collect data only for specified, explicit and legitimate purposes described in the business's privacy policy, marketing materials, and just-in-time notices (such as the California Consumer Privacy Act's notice at collection); and
2. Further use the collected data only for a purpose compatible with the specified, explicit and legitimate purposes.

In addition, we do have a bit of guidance to rely on. First, the FTC reminded companies in 2020 that failure to practice purpose limitation is an unfair or deceptive practice under Section 5 of the FTC Act and actionable by the FTC. For example, claiming collection of data for security purposes but ultimately using it for advertising purposes is an incompatible use and a failure to practice purpose limitation.

Second, while *some* marketing may not be compatible with the primary purpose, the California Consumer Privacy Act (CCPA) regulations and the regulatory commentary in the California Privacy Protection Agency's (CPPA's) Final Statement of Reasons leads us to believe that California regulators intended to preserve a business's ability to engage in marketing for related products or services.

Third, consider the chart below, which describes what a few regulatory bodies have listed as factors to consider when determining compatibility

| FACTORS TO BE CONSIDERED | GDPR* | EDPB** | UK*** | CO***** | CA**** |
|---|---|---|---|---|---|
| The type, nature and amount of data the business seeks to process for the new purpose | x | x | x | x | x (RE) |
| The type and degree of possible consequence or impact to the consumer of the new processing purpose | x | x | x | x | x (RNP) |
| The existence of additional safeguards for the data | x | x | x | x | x (RNP) |
| Whether the business practiced data minimization****** | x | x | x | x | x (RNP) |
| The reasonable expectations of the consumers as to their further use | x | x | x | x | x (C) |
| The link between your original purpose and the new purpose | x | x | x | x | |
| The context in which the data was collected | x | x | x | x | |
| The relationship between the consumer and the business | | | x | x | x (RE) |
| Whether the involvement of service providers, contractors, third parties or other entities in the collecting or processing of data is apparent to the consumer | | | | x | x (RE) |
| The source of the data and the business's method for processing it | | | | | x (RE) |
| The specificity, explicitness, prominence and clarity of disclosures to the consumer about the purposes for processing their data | | | | | x (RE) |
| The strength of the link between the reasonable expectations of the consumer and the further use of personal data | | | | | x (C) |

* The General Data Protection Regulation states these factors shall be considered.

**The European Data Protection Board has not adopted the European Commission's working paper on purpose limitation that lists these factors but states these factors may still be relevant. (See footnote 34. edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (europa.eu)).

***The Information Commissioner's Office states these factors should be considered but notes the list is not exhaustive and other factors may be considered. (See generally ICO purpose limitation guidance. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/).

****The CPRA regulations state these factors shall be considered. Also, please note, while all of the CPRA factors listed above should be assessed together to determine compatibility, the CPRA regulations break out the factors into three different buckets: specifically, what factors (i) meet the "reasonable expectations of consumers" (RE); (ii) are "compatible" (C); and (iii) are "reasonably necessary and proportionate for the disclosed purposes" (RNP).

*****The Colorado rules state these factors may be considered. (See CPA Rule 6.08 (Secondary Uses) https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf).

******Data collected in violation of the data minimization requirement will work against any argument for compatibility

Based on the above guidance, if a business clearly communicates to consumers what data it is collecting, communicates the specific and identifiable business purposes (primary and compatible) for collecting the data, and directly collects the data from the consumer (as opposed to collecting it from another source), and if a strong link exists between the reasonable expectations of consumers and other disclosed purposes, there is a decent argument, supported by the CPPA, that the other disclosed purposes are compatible with the primary purpose for collection. (Advertising and marketing is not explicitly listed as an incompatible purpose under the CCPA, the CCPA/CPRA regulations, or the CPPA's Final Statement of Reasons. The CPPA instead takes the position, in its Final Statement of Reasons for the CPRA regulations, that whether a purpose is compatible should be determined by the "objective" purpose limitation factors set out in the CPRA regulations. See subparagraph (B) under the section titled "Changes Made to Article 1. General Provisions" (https://cppa.ca.gov/regulations/pdf/20230329_final_sor.pdf )).

## What Goes into a Compatibility Manual?

Given the complexities of compatibility, each business must develop a procedure or manual for evaluating, assessing and determining whether a use case can be characterized as "primary," "compatible" or "incompatible."

To better assess compatibility, first and foremost, if you aren't data mapping, start to do so. It is time- and resource-consuming, yes, but it goes a long way to developing a viable privacy compliance framework for your business.

After you data map, taking into account any jurisdiction-specific factors (such as those identified in the chart above), ask the following questions for each separately identified data use:

1. **At the time of collection, did we disclose the data elements, the sources of the data, our primary purpose for collecting the data, and any other disclosed purpose to the consumer?** Transparency in the consumer-facing touchpoints typically supports a favorable analysis regarding the compatibility of using the collected data for "another disclosed purpose" (i.e., compatible with the primary purpose).
2. **Are the other disclosed purposes related to the primary purpose? If they are not related, it will be extremely difficult to argue compatibility.** For example, if a business collects the data to provide a connected device service and the business consistently discloses that it will use the data for the additional purpose of marketing other related services or features, the business has a colorable argument that "marketing" the additional related service or feature is compatible.
3. **Is there a strong link between the consumer's expectations and the use of the data for the other disclosed purpose?** Specifically, consider:
   - The business's relationship (or lack thereof) with the consumer.
   - Whether the average consumer would be surprised to learn the data they provided for one service is now being used to market a different service or product from the same company. If words like "unexpected" or "unconnected" or "unnecessary" or "unrelated" or "unjustifiable" come to mind when considering a "compatible" purpose, it is likely incompatible.
   - What does a consumer intuitively understand about the business from which they are purchasing a product or service and then sharing their connected data with? Would a consumer reasonably understand their data may be used in this other manner (e.g., to market another product or service)? (Recall that the CCPA permits the use of data to provide "marketing and advertising services," excluding cross-contextual behavioral advertising.)
   - From what source did the business obtain the data? If the data was collected from a source other than the consumer (or the source is not apparent to the consumer), the compatibility argument decreases because the consumer is not aware of the data collection.

If a use case is not compatible with the primary purpose, express affirmative consent must be obtained before the business can use the data for the incompatible purpose. If the use case develops after the original date of collection and is determined to be compatible, the business must provide effective, transparent notice and an ability to opt out of the newly created compatible purpose before it becomes an active use case.

It is also important to note that once data is truly de-identified it is no longer protected data under the data protection laws, and thus, we do not have to be concerned about using de-identified data for any number of purposes, including improvements and interventions in public health, disease prevention and management, urban planning and infrastructure development.

## A Case Study – Wearable Fitness Trackers

The primary purpose for the collection of data from wearable fitness trackers is to monitor and assess various aspects of an individual's health and fitness. Wearable fitness trackers are designed to track and record data related to physical activities, sleep patterns and other health metrics. The key purposes for collecting this data include:

**Health monitoring** of vital signs such as heart rate, blood pressure and sometimes even ECG data. This information provides insights into an individual's overall cardiovascular health.

**Activity tracking,** including the number of steps taken, distance traveled and calories burned throughout the day. This data helps users set and achieve fitness goals, promoting a more active lifestyle.

**Sleep analysis** using sensors to monitor sleep patterns, including sleep duration and quality and different sleep stages. Understanding sleep patterns can help users improve their sleep hygiene for better overall health.

**Exercise performance tracking,** including the pace, distance and duration for different types of exercises, such as running, cycling or swimming, helping users optimize their workouts.

In this case, the primary purpose centers on individual health monitoring and improvement. Consider whether offering and marketing tailored services related to health are compatible purposes. If disclosed, such services could include personalized coaching and recommendations, introducing personalized gamification elements to make the fitness journey more engaging, developing and offering adaptive training programs targeted at specific users based on their connected data, or nutritional guidance services reliant on integrating data from wearable devices with nutritional information to offer personalized dietary guidance.

A business must work through a compatibility test for each of these examples of "other disclosed purposes" to determine whether they are compatible. For example, before using primary purpose data to offer individualized coaching and recommendations, one could run through the questions in the compatibility manual above, taking into account any other jurisdiction-specific factors. Otherwise, a business may be in the position of processing data for purposes that actually require consent, putting the business not only in regulatory noncompliance but often contractual noncompliance.

**Conclusion**

As is often the case in privacy matters, there is no bright-line rule to follow regarding compatibility. To be compatible or not to be compatible is still the question. Each business has to answer that question for themselves (again and again). However, as regulators ramp up their enforcement actions, we will learn more about how the compatibility factors should be interpreted. In the meantime, we hope the above manual provides a commonsense approach to answering the question: To Be Compatible or Not To Be Compatible?

## Related Professionals

Allison Cohen . . . . . ahcohen@loeb.com
Teodoro "Teddy" Shelby . . . . . tshelby@loeb.com