Consumer Technology Association™

CTA's Guiding Principles on the Privacy and Security of Personal Wellness Data

I. Introduction

Wellness-related wearable devices represent one of the fastest-growing segments of the Internet of Things. Consumers now harness data about themselves—calories, steps, heart rate, and more—to improve their well-being. In the future, these devices will tell consumers even more about themselves, providing analytics and insights that will empower them to lead richer and healthier lives. Society also will benefit as we develop sophisticated tools to research health and wellness on an aggregated basis.

All of these benefits depend on the collection and use of data, some of which can be considered personal or sensitive. Companies in the health and fitness ecosystem understand that they must be good stewards of that data to maintain consumer trust.

With trust in mind, these Guiding Principles ("Principles") articulate the Consumer Technology Association's ("CTA") recommendations for voluntary best practices that mitigate risks that consumers may perceive with respect to personal wellness data.[1] These Principles articulate practices that can be followed by a broad variety of companies in the health and fitness wearable ecosystem. If adopted, they may help companies obtain and maintain consumer trust. Since the Principles are baseline recommendations, companies following them will retain flexibility on how to implement them, accounting for each company's unique combination of products, services, and users.

Data privacy and security are continually evolving concepts that require a dialog among companies and consumers. As consumer preferences and comfort with technology evolve, so too will companies' products and services. CTA encourages companies to maintain an ongoing dialog with consumers to both discuss the potential value of health and fitness technologies and the privacy options such technologies offer and also to understand their potential sensitivities about the use of this data.

[1] These Guiding Principles are recommendations that a CTA working group has developed for voluntary best practices. They are not intended to supplant rules developed for doctors and other healthcare professionals under the Health Insurance Portability and Accountability Act (HIPAA). Nor do they represent a negotiated, industry-wide self-regulatory code of conduct.

Text last updated Oct. 20, 2015

The Principles begin by defining key terms. Next, we list each principle and the issue it attempts to address. We then offer a more complete discussion of each principle. CTA intends to review this document on a regular basis in concert with its members to ensure that it accurately reflects current data privacy and security concerns.

II. Definitions

Company.

Any person, including corporate affiliates, that manufactures a device, develops software, or provides a service that collects, stores, or uses personal wellness data. As used in this document, company refers to the entity providing a product or service to the user, not the software or hardware platform on which the product or service may rely.

Unaffiliated Third Party.

Any person other than (1) a user of a company's products or services; (2) a company's employees; or (3) a vendor or supplier to a company when such vendor or supplier is used to provide a product or service related to personal wellness data.

User.

A consumer who uses a company's product or service and from whom a company collects personal wellness data in connection with that product or service.

Personal Wellness Data.

Wellness data that a company collects, stores, or uses about an identified user through a device, software, or service that is primarily used to collect wellness data. However, data that has been reasonably de-identified[2] is not personal wellness data and therefore is not covered by these Principles.

[2] De-identification of data—removing information from data that could reasonably be used to identify an individual person—is a subject of intense debate. These Principles do not endorse any particular method of de-identification or set a standard for when data has been adequately de-identified. Instead, companies should use their expertise, taking into account the type and use of personal wellness data and using the technical tools available to them, to determine how to de-identify such data.

III. Principles to Address Privacy and Security Risks

Security

Robust security measures are the foundation of good data management. While consumers have access to many tools that allow them to secure their data, companies must do their part to secure personal wellness data from the outset.

A company should secure personal wellness data by deploying measures that are reasonable and proportional to the sensitivity of that data, taking into account that consumers generally have heightened expectations of security with respect to personal wellness data. Companies should make arrangements with their vendors or suppliers who may handle personal wellness data to secure it using reasonable administrative, physical, and technical safeguards.

Policy and Practice

Consumers need to understand how personal wellness data is handled to be comfortable using health-related devices and services.

A company should have a clear and easily understood written policy for collecting, storing, using, and transferring personal wellness data. That policy should reflect broadly recognized fair information practice principles, address reasonably foreseeable security risks, and ensure compliance with applicable laws.

Concise Notice

Consumers may be unable to understand lengthy privacy policies, which would impede their ability to understand how personal wellness data is collected and used.

A company should make publicly available a summary of how it collects, stores, uses, and transfers personal wellness data. Companies are encouraged to provide these summaries in creative formats and through accessible methods that facilitate rapid learning, such as graphics, icons, charts, video, or audio.

Unaffiliated Third Party Transfers

Consumers seek transparency about and sometimes want to control personal wellness data transfers among companies.

A company should obtain affirmative consent before transferring personal wellness data to an unaffiliated third party, unless otherwise required by law or the company discloses in its privacy policy circumstances, such as emergencies, in which notice is sufficient. A company need not obtain affirmative consent from the user for subsequent personal wellness data transfers to the same unaffiliated third party, unless the type of personal wellness data to be transferred materially changes or the unaffiliated third party indicates a material change in the purpose for which it will use such data. Users should be able to revoke consent for the company to continue transferring personal wellness data to unaffiliated third parties at any time, unless otherwise required by law. A company should notify users if revoking consent will disable certain functions of a product or service.

Fairness

Personal wellness data collected from Internet of Things devices, combined with new data analytics, can provide many consumer benefits. Analytics can help consumers learn more about their health, enable them to reach their goals, and produce socially useful outcomes. Companies need to guard against the possibility that data analytics unintentionally could create unjust or prejudicial outcomes for consumers. While CTA is not aware of any such outcomes, this principle, which is inspired by existing U.S. federal, anti-discrimination laws, guards against that possibility throughout the lifecycle of their products.

A company should not knowingly use or disclose personal wellness data in ways that are likely to be unjust or prejudicial to consumers' eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance.

Companies are encouraged to periodically review algorithms or automated decision methodologies that use personal wellness data to guard against the possibility that they could create unjust or prejudicial outcomes for different categories of consumers.

Personal Data Review, Correction, and Deletion

Consumers wish to manage personal wellness data carefully. The ability to review, correct, or delete personal wellness data permits consumers to guard against inaccuracies or dissemination of the data beyond their control.

A company should provide a user with a means to review and correct the company's stored personal wellness data if the company intends to share it with a third party that will determine the user's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance. A company need not give a user the ability to review or correct personal wellness data if the user already has a means to do so.

A company should give a user the ability to request the deletion[3] of that user's personal wellness data and grant that request to the extent: (1) that deletion is technically, economically, and legally feasible, (2) that the company can attribute personal wellness data to the requesting user, and (3) that the user does not already have the ability to delete his or her personal wellness data. If a company transfers a user's personal wellness data to its vendor, supplier, or other service provider, that company should make technically, economically, and legally feasible efforts to promptly notify the transferee(s) that a user has requested deletion of his or her personal wellness data. Companies are encouraged to include in their contracts with vendors, suppliers, or other service providers a requirement that such transferees delete personal wellness data upon receiving notification from a company when technically, economically, and legally feasible.

Advertising Communications

Advertising is a useful tool that facilitates communication between companies and consumers. However, consumers want to control how personal wellness data is used for that communication.

A company that tailors advertising based on users' personal wellness data should provide users with the ability to opt out of such advertising.

[3] Deletion could mean either (1) erasure of the data or (2) removing information from data that could reasonably be used to identify an individual person. Such deletion should occur in a reasonable period of time reflective of the technical infrastructure at the company (for example, whether the company maintains personal wellness data on disaster recovery systems).

Consistent with the Unaffiliated Third Party Transfers Principle, a company should obtain affirmative user consent before knowingly transferring personal wellness data to unaffiliated third parties who intend to use it for their own advertising purposes.

Law Enforcement Response

Consumers and companies alike are concerned about government access to personal wellness data. While companies must comply with legal process, they can be transparent with consumers about when and how they respond to lawful requests for data.

A company's privacy policy should describe how it responds to requests for users' personal wellness data from federal, state, local, or foreign law and civil enforcement agencies.