asae foresightworks

Who Owns The Data?

SUMMARY: In the United States, there is a growing movement among technologists and consumers to give individuals more control over data about themselves (their identifying information, online communications, purchasing histories, social media habits, etc.). This idea may prove a challenge to existing industry models, as free consumer data is the lifeblood of many popular online services and programs, particularly mobile applications.

Forecasts

- The battle for control of personal data could involve consumers less and less. As government regulations on use of consumer data are relaxed, it will be corporations challenging other corporations for access to consumer databases, with users having little say.
- Current methods for enabling consumers to control their data are incomplete and cumbersome. As this idea grows, new ways of data sharing and control could arise. These may include differential controls, allowing the release of some data (consumer preferences) but restriction of other data.
- User concerns about data privacy could drive behavior changes and product innovations, including interest in products in which user data capture is ephemeral. Users may also begin to purposely create public-facing consumer personas that are similar to, but not exactly like, their actual selves.
- The issue of who owns consumer data could escalate as connected devices spread (the internet of things) and collect more consumer data, often surreptitiously.

Key Uncertainties

Convenience of data ownership systems

•

The role of regulation

•

Discontinuous data disasters

•

Evolving privacy concerns

•

Availability of non-data models of funding consumer access

•

Tech industry views of security

2018© ASAE Foundation

Supporting Trends

- **Who controls data trails?** People are generating vast data trails of personal information, leading to growing questions about who should own and control that data.
- **Wearable technologies.** Wearables will continue to grow and will expand into new domains like payment and health monitoring.
- **Predictive analytics.** Companies are adopting predictive analytics to turn their data into anticipatory knowledge.
- **From big data to fast data.** Increasingly, the value from big data is coming from just-in-time use. "Fast data" emphasizes real-time decision making based on the idea that the greatest value from data comes when the analytics can be used immediately.
- **Cybersecurity.** Digital infrastructures face risks from increasingly sophisticated criminal hackers, non-state actors, and growing international cyber-warfare capabilities. Rapid expansion of the internet of things (IoT) is exacerbating the problem, bringing online millions of new, weakly secured devices.
- **Mobile phone data for social research.** Researchers are using datasets of mobile phone usage to study a wide range of human behaviors.
- **Concern about online privacy.** Americans are worried about the privacy of their personal data online.

Related Drivers of Change

- Fast Data
- Dark Data Comes to Light
- Personalized Artificial Intelligence
- Anticipatory Intelligence

Notable Data Points

CYBERSECURITY

80% of common IoT devices **have inadequate password protections,** and 70% do not encrypt data during transmission.

Source: Hewlett-Packard

WEARABLE TECH

By 2021, it is estimated that **29% of Americans will own and use** a wearable device.

Source: Forrester, Tractica

INTERNET OF THINGS

Growth for the IoT is forecast to be rapid: IHS forecasts that the IoT market **will grow from 15.4 billion devices in 2015 to 75.4 billion in 2025.**

Source: IHS Markit

2018© ASAE Foundation

Strategic Insights

- Associations and organizations will need to be aware of changing responsibilities for holding member data as these issues evolve. Having a clear—and clearly communicated—policy on data collection, release, and use could allay members' concerns about their data privacy.
- An increasing threat to data privacy and security is data "leakage" from poorly designed or secured apps and software used for organizing or connecting with members. Even if organizations are not directly responsible for these leaky apps, they may still be on the hook for leaks they generate.
- Similarly, association leadership should be aware of members' collective views on data privacy and use. What is allowed by law or regulation may differ from members' own desires.
- Associations have a lot of potentially lucrative consumer data and should consider ways to monetize it. The trick will be to do so judiciously within the strictures discussed above.
- International data-protection standards are diverging, making this a growing issue for international associations. Consumer privacy in Europe, for example, is highly valued and protected. This leads to potential issues on both the organizational level and the individual member level.

Timing

- **Stage:** Emergent, though its importance is growing as consumer awareness spreads
- **Speed:** Spreading at moderate speed, though occasionally accelerated by public interest events—e.g. data breaches

Potential Alternative Futures

- **Consumer rebellion:** Tired of their data being used without compensation and concerned about privacy, consumers rise up, using ad hoc methods and boycotts to halt the flow of data while also demanding tighter government regulations on data use and monetization.
- **Bad data:** Data become less reliable or valuable for companies due to purposeful spoiling, spoofing, or masking by users.
- **Breach exhaustion:** Faced with what seems like a never-ending series of consumer-data privacy breaches, data ownership and privacy are no longer an issue for consumers, who see attempts at data security as pointless.

2018© ASAE Foundation

Take Action

- **Establish standards and best practices around data ownership.** Associations are in a privileged position to negotiate with multiple stakeholders and government to bring order and standard practice where few safeguards exist now. They also can clarify any member preferences and openness to sharing data for mutual benefit. Organizations may soon have to demonstrate they offer appropriate safeguards.
- **Equip members to educate customers and clients about their data rights.** Few people understand the value and risks associated with their personal data. Associations can help professionals and businesses explain the benefits and trade-offs of disclosure.
- **Protect sensitive industry data from misuse.** Most industries have some sensitive consumer or business data that law enforcement, regulatory agencies, and research organizations want to access. Associations can advocate for protective laws and regulations and educate members about their rights and responsibilities in handling this information.
- **Track how other countries resolve data ownership issues.** The European Union and some other countries have more restrictive policies related to consumer data than the United States. Trade associations representing data-rich industries need to stay on top of these regulations; others can monitor these developments to anticipate how these issues might be resolved.
- **Protect your data assets.** Every association knows something others want to know. Member and research data are valuable assets others want to use. Associations should have clear policies and smart business practices that define and restrict use to appropriate purposes. Some member data such as ethnicity and sexual orientation could be sensitive. While you could keep vast amounts of transaction data, you may choose not to retain some data beyond its immediate purpose to protect your members and staff.

Keyword Search

To continue researching this change driver, use these search terms: ***privacy, personal data, data mining, big data, security, data trails, data exhaust, privacy breach, cybersecurity security, wearables, online privacy, public data infrastructure, application programming interface, API***MEETING TERMS: ***event, meeting, conference***

Who Will Be Affected

Associations in data-rich industries, especially those handling extensive consumer data, are at the forefront of data ownership issues. Many associations already aggressively police copyright and intellectual property ownership issues in their conference presentations, journals and publications, and social media. The source and ownership of data will become part of that monitoring.

About ASAE ForesightWorks

ASAE ForesightWorks is a deliberate, evidence-based research program and emerging line of products to provide association professionals with a *continual* stream of intelligence about the changes facing the association industry, including:

- regularly updated action briefs;
- tools for applying insights from the research in your association;
- guidance in performing environmental scans; and
- opportunities to engage with peers around the research.

Ultimately, the program's mission is to empower association leaders to create a culture of foresight in their associations and to lead their organizations confidently into the future.

Check **asaecenter.org/ForesightWorks** and follow **@ASAEfdn** on Twitter for updates on new findings and events.

2018© ASAE Foundation