Deloitte.

Data ownership, privacy & collaboration

when the lines between the physical and digital worlds are blurring

Deloitte in collaboration with Wiliot, October 2020

Contents

1. Executive Summary

Cheap and battery-free Bluetooth-enabled tags with advanced sensor capabilities can fully automate data collection. This enables a plethora of use cases that up till now have not been feasible, viable, and desirable. This raises the question of how the challenges around data privacy, data ethics, and data exclusivity can be addressed?

The emergence of Bluetooth-enabled tags the size of postage stamps with advanced sensor capabilities makes it possible to fully automate data generation and collection. This enables a plethora of use cases that up till now have not been feasible, viable, and desirable[1].

However, concerns relating to data ethics, data privacy, and data exclusivity for competitive reasons may hamper collaboration between participants in the supply chain and their pursuit of shared benefits, especially in the form of a more data-driven retail experience in response to the ever-growing focus on increasing share-of-wallet.

To address these concerns, this paper attempts to answer the following questions:

- Who owns the data generated by a tag?
- Which claims, if any, does the producer/manufacturer, retailer, logistics provider, or any other supply chain participant have on data generated by the other participants?
- Which types of data will the tag be able to collect that are either sensitive, private, or otherwise restricted by regulations?
- What incentivizes tag owners to share data?

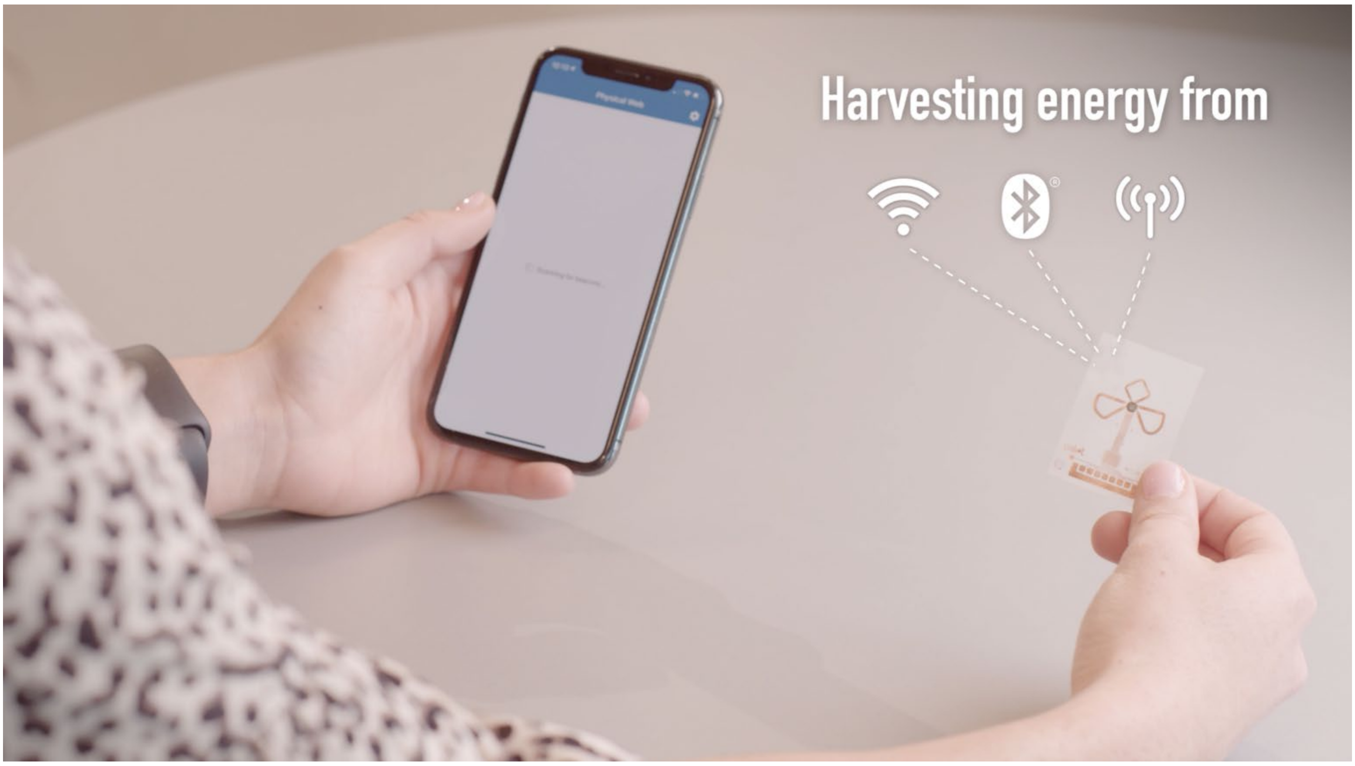
This paper proposes the following design principles in response to the above concerns:

- Whoever owns the tag owns the data.
- Access to and ownership of (historic) sensing data should be determined by product characteristic.
- Consumers have to opt-in to use the tag they own.
- Companies must have clear ethical standards to build the trust required to allow the collection of data.

“It’s been more than 20 years since the idea of the internet of things was first conceived, but till now, it’s really been the internet of expensive things.”

Stephen Statler
Wiliot

[1] https://podcasts.apple.com/us/podcast/5-affordable-battery-free-iot-chip-possibilities-are/id1485697579?i=1000477550175



Wiliot tags harvest radio frequency waves to power a nano-watt wave compute cycle.[2]

2. New technology creates new opportunities

2.1. A new category of IoT devices emerges

Cheap, battery-free, active Bluetooth-enabled tags make up a new category of IoT devices that overcome several factors otherwise inhibiting widespread adoption: cost, size, connectivity, and environmental concerns. The cost and size of Wiliot's active tags are expected to be on a level with passive RFID tags at pennies rather than the dollars as they leverage the same production infrastructure.

Moreover, Wiliot's active tags remove the need to excite passive RFID tags with a manual scan, and they replace the environmental concerns of discarded battery-powered active tags with an ability to recycle the radio waves that surround us.

Unlike a passive tag requiring excitation by an external scanner held by an employee or consumer to collect data and transmit them, an active tag is always on. This allows light, humidity, proximity, and weight sensors on the active tag to harvest data about the thing it is attached to throughout its lifecycle.

[2] https://support.wiliot.com/hc/en-us/articles/360023549753-Nano-Watt-Computing-An-Overview

2.2. Battery-free active tags can bring products to life

The effect of a smartphone computer in the pocket of every human connecting everyone on earth was immense[3] with entire industries and multiple Fortune 500 companies built on top of it[4]. The implications of similarly connecting every product or thing by tagging it with a computer could be equally or more transformative. Paraphrasing Benedict Evans[5] "Software is eating the world and with most people and services now online, money and products (harder, more tangible markets) are next."

Some of these benefits will materialize in the form of cost reductions through better supply chain visibility, traceability, inventory management, fraud reduction, etc. Other benefits will drive top-line growth through either better existing products and services or completely new value propositions. The always-on data harvest from products continuously connected to the internet throughout their lifecycle may even bring about demand chains[6] as a paradigm shift away from supply chains. In demand chains production would shift from forecasts to a process informed by real-time demand signals extracted from the data harvest.

A demand signal could be as simple as a potential buyer picking up a product in a store, indicating consideration of a purchase that may be influenced. It could also be a signal post-purchase indicating not just satisfaction with the product but also usage patterns.

Yes, brands already have visibility into purchases of their products, and so do retailers. However, this information typically comes after a delay (sometimes a delay of weeks), and it lacks the kind of context that one may enjoy from observing first-hand how positioning, pricing, and promotion can affect not just purchases, but consideration of a purchase.

Yes, the large platform players (Google, Amazon, Facebook, Alibaba, etc.) can infer similar metrics and ultimately determine and drive purchase propensity through their algorithms, but not all this information is within reach for brands and retailers.

As such, demand signals from cheap, always-on, active tags the size of postage stamps blur the lines of between the physical and the digital world. This allows insights into the physical world of retail in a way that is different from data captured by the large platforms in several critical ways:

1. Demand signals are real-time and context rich.
2. Demand signals concern the product, not the user, as the data is ultimately owned by either the buyer or the seller, not the intermediating platform.
3. Demand signals continue, depending on whether the tag is situated on the package or the product, post-purchase.

Passive tags (typically RFID, QR, barcodes) cannot collect or transmit any data without being scanned or charged using an external scanner.

Active tags (powered either with or without a battery) can collect and transmit data for as long as they have enough power.

[3] https://www.theatlantic.com/technology/archive/2017/06/the-iphone-was-inevitable/531963/
[4] https://stratechery.com/2018/the-bill-gates-line/
[5] https://a16z.com/2018/11/16/summit-2018-benedict-evans-annual-keynote/
[6] https://www.youtube.com/watch?v=PpW9UDjE8d4

2.3. Immense sensing capabilities come with great responsibilities and ethical complications

Knowledge is power and by extension, so is data. Information asymmetries have consolidated market power on the once open web to a handful of corporations with rising criticism of the way these data are monetized through behavioral futures.[7]

Consequently, the potential business, privacy, and ethical complications of the fully automated data harvest from always-on active tags on nearly everything must be considered as they are likely far-reaching.

"Once the product goes to the consumer, you tend to lose touch. With this, you can keep knowing what happens with it. "

Robert Schmid
Deloitte

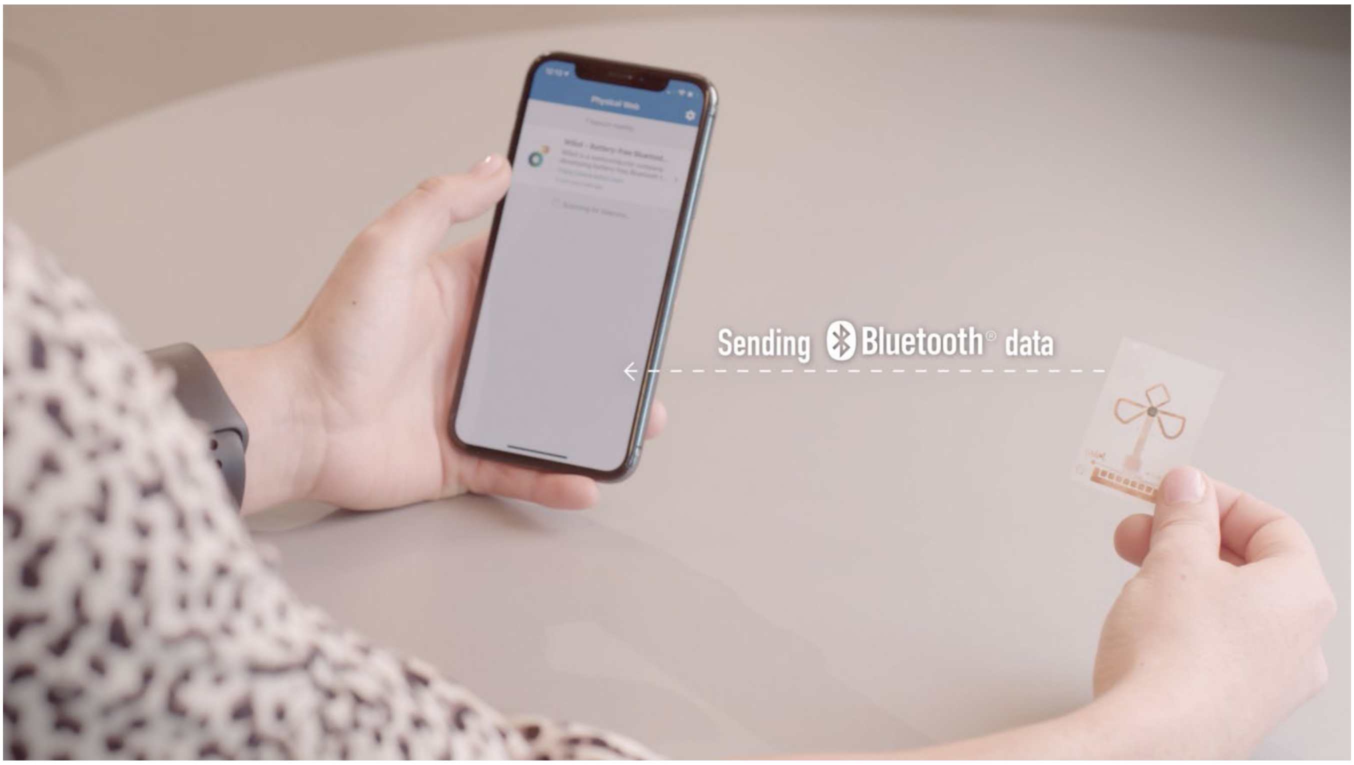
Data ethics

Data ethics is the ethical dimension of the relationship between technology on one side and the civil rights, legal certainty, and basic societal values, which the technological development gives rise to, on the other. Data ethical considerations include, without being limited to, what kind of data the company uses and how the data are provided (e.g. consumer, production and behavioural data). Furthermore, it considers which ethical assessment has been applied to the business model if the company sells consumer data to third parties and which processes are in place to ensure that data ethical issues are continuously being discussed and handled within the company.

Essentially, the following questions must be considered:

- Who owns the data generated by a tag?
- Which claims, if any, does the producer/manufacturer, retailer, logistics provider, or any other supply chain participant have on data generated by the other participants?
- Which types of data will the tag be able to collect that are either sensitive, private, or otherwise restricted by regulations?
- What incentivizes tag owners to share data?

[7] https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook



Wiliot tags broadcast encrypted Bluetooth advertising packets.

3. New use cases with shared benefits become possible but may involve personal identifiable information

3.1. Collaboration is required to realize shared benefits

The application domains for a cheap, always-on active tag are numerous and will span across manufacturing, supply, sales, ownership, and recycling. Moreover, the use cases for durable goods are likely different from those of consumables, and certain cases may even warrant tagging the product itself over the packaging. This span of use cases is unlikely to have the same data collection requirements, ownership changes, and regulatory regimes. However, much can be learned from considering the lifecycle of a bottle of gin as an example:

Step #	Use case step	Manufacturer	Retailer	End consumer
1	The gin is bottled, and the tag is attached to the label.	Can I optimize my inventory?	Can I expect to receive the volume I ordered?	Where does this gin bottle originate from; is it safe and legal to buy?
2	While en route to the retail store, the tag reports its position and temperature.	Can I optimize my warehouse and logistics operations?	Can I source this gin smarter and create a more resilient supply chain?	Is the quality of this gin as advertised?
3	Once in the retail store, the tag reports its position and proximity indicating a level of attention.	Is the current shelf location for the gin bottle worth the money?	Can I optimize the shelf layout?	Where do I find this gin bottle that I've received an offer for?
4	Once bought by the end consumer, the tag reports proximity and position indicating usage and eventual discarding.	How is the end consumer using the gin bottle?	How can I optimize orders to the manufacturer to match end consumer demand?	Where is my gin bottle; can my bottle be replenished automatically before I run out?

Table 1 - Use case example

Additional scenarios and use cases could be considered. Some would focus on solving existing operational problems better and cheaper; some would focus on improving the value propositions of existing offerings, while yet other ones would address jobs no one has yet considered, similar to how no one had thought of Uber at the time the iPhone launched. In any case, while some use case steps require data that are purely operational, others require more sensitive data:

- Operational data with no or little competitive value (steps 1-2).
- Operational data with competitive value (step 3).
- Personal identifiable information (step 4).

It is worth noticing that there are a couple of situations where the interest of different participants could be running counter to each other, including, without being limited to:

- Should the retailer, who's running out of stock, be allowed to verify through the manufacturer's data that the gin bottle is en route?
- Should the manufacturer, who's wondering whether the current shelf position is priced right relative to the demand it is generating, be allowed to tap into the retailer's proximity data indicating purchasing intent in order to optimize supply to match demand?
- Should the end consumer be allowed to verify the provenance and quality of the product through its historic position and temperature data?
- Should the manufacturer or retailer be allowed to tap into gin bottle usage by the end consumer to develop products tailored to that consumer's drinking habits?

However, these pale in comparison to the benefits that could be realized if data were shared between the participants. While the list above outlines areas of potential diverging interests, it also highlights opportunities for significant operational improvements for all involved parties. One can only imagine how better data collection and sharing might make retail more competitive versus the data-driven e-commerce alternative that inherently combines both consumer data (propensity to buy) and operational data (available goods and delivery times).

"This kind of device-based serialization makes it possible to create a digital twin allowing a physical product to have a digital identity and communicate throughout its journey."

Rasmus Winther Mølbjerg
Deloitte

3.2. Tightly regulated personally identifiable information is required for some use cases

When it went into effect in 2018, the European Union's General Data Protection Regulation (GDPR)[8] offered ground-breaking protections for personal data. California's Consumer Privacy Act (CCPA)[9] had a similar, far-reaching impact, and multiple similar regulations are expected to follow in other jurisdictions.

The starting point for the GDPR and other similar regulations is the concept of personal data.[10] Personal data makes it possible to, directly or indirectly, identify a natural person. Most people are aware that a name, an address, or an email address are personal data, but IP addresses or device IDs are also considered to be personal information. Furthermore, a distinction is made between 'regular' personal data and 'special categories of personal data'.[11] A third complicating factor is that the GDPR also applies when data are indirectly traceable to a person. Data could appear not to be personal data at first sight, but in combination with other data or a particular context, they can lead to an individual and are thus personal data.

Pseudonymized or anonymized data are often assumed not to be personal data. This is incorrect with regards to pseudonymized data, where GDPR is explicitly applicable. However, if a dataset is anonymized, then the GDPR is no longer applicable. In order to obtain full anonymization of pseudonymized data, the key discarded, and all data that can be redirected to a person eliminated to make the encryption irreversible. That last criterion is very rarely fulfilled. In most cases, a dataset contains combinations of data for it to be useful or interesting. Often it is this combination that can still lead to an individual.

Moreover, the privacy rights of individuals covered by GDPR mustn't be diluted if data is transferred to third countries outside the EU[12].

GDPR roles and responsibilities

GDPR introduces the roles of both a data controller and a data processor, who collectively own the responsibility for the personal data being processed.

The Data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data i.e. what personal data is collected, why and who is it shared with.

The Data processor is the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[9] https://oag.ca.gov/privacy/ccpa
[10] https://www2.deloitte.com/ch/en/pages/risk/articles/the-gdpr-areas-of-attention-and-practical-guidance.html
[11] https://datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger
[12] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

4. Design principles for collaboration on data sharing are necessary

4.1. Collaboration is required to realize shared benefits

The use case steps presented in table 1 show how different participants in the supply chain could get significant benefits from harvesting additional data about their operations and consumers, and that controlling and processing these data (while not out-of-bounds) is likely to be regulated. Consequently, the question that remains is which design that best balances data ownership, regulatory requirements, and incentives to share data based on mutual benefits.

On one end of the spectrum is the scenario where every participant in the supply chain decides to add its own tag to any given product and not share any of it. In some ways, this is similar to the current state where various supply chain participants add their own RFID or barcode to any given product to enable the serialization required by their operations. While this allows full control and exclusivity to data that any given participant can collect, it also limits data that can be collected to the point that very few, if any, of the use case steps above are possible.

On the other end of the spectrum is the scenario where all participants in the supply chain agree to collaborate and share data collected from a single tag. Primary ownership of the tag and the data it generates would change hands along with the product as it is passed on to the next participant in the supply chain. While this allows access to all data from cradle to grave, it also comes with significant coordination cost and regulatory challenges as the purpose of collecting a specific piece of data may not be evident to the tag owner.

Clearly, both scenarios are unsatisfactory. What is needed is a set of principles that provides a balance between the two extreme scenarios, where continuous data collection throughout the supply chain is made possible, where data privacy and regulatory compliance are feasible but not obstructing, and where data exclusivity is possible for competitive reasons but not a hindrance for collaboration for common benefits.

4.2. Design principle 1: “Whoever owns the tag owns the data“

This principle borrows the core concept of creating financial value and accountability. If you own the resources, you own the outcome of those resources; hence the ownership of the tags provides ownership of the data. Even though this principle seems trivial, the introduction of search engines, social media platforms, and e-commerce platforms make data ownership a subject that is paramount to manage if you want the consumers’ trust.

4.3. Design principle 2: “Access to and ownership of historic sensing data is determined by product characteristics”

Active tags (working in conjunction with a cloud solution) provide the possibility for things to have a memory of the past. This raises new questions about how information about the product’s past is passed along. Depending on the use case, the need for passing on this product history varies. As an example, when a consumer wants to buy a used car, she would like to know the history of the car with all the details since that will remove the information asymmetry between the buyer and the seller. However, there might be use cases where there is no need nor desire to share that information. In other words, it needs to be the owner of the tag who decides whether the new owner has access to the history of the tag, which in turn also creates an opportunity for new pricing mechanisms.

4.4. Design principle 3: "Consumers have to opt-in to use the tag ID they own"

There is not much debate about whether consumers need to opt in to sharing this kind of data. GDPR and CCPA regulations are unambiguous. However, building trust between brands and consumers is still an important issue. Brands need to provide the opportunity for their consumers to remain in control of their data. A study conducted by Deloitte and Ahold Delhaize asking 15,000 European consumers[13] found that consumers' willingness to share data is correlated to which type of institution they engage with. Providers of medical services, government agencies, and grocery retailers are the top 3 in that order. This finding is not surprising. However, the need to provide consumers with control and act ethically is an important element. Therefore, even though consumers trust retailers as a data custodian, there is a need to ask for permission to use the data collected with tags. The same study also showed that there is no uniform 'European consumer' since the local variations between countries were significant, which also indicates the need to be able to localize future solutions.

4.5. Design principle 4: "Clear ethical standards must guide the collection of data"

Consumers should be able to trust that the way organizations use their data is not just transparent and in line with regulations; it is also ethical in a broader sense. This means only using data in the context for which consent has been provided by the consumer, even though it might be tempting for retailers and other data-rich organizations to make large data enrichment models with a commercial mindset to earn more money. Organizations will need to become transparent about their governance, guiding principles, and practices in dealing with consumer data. It will also mean giving a voice to the consumers and even helping consumers understand what they should expect from organizations when it comes to data ethics.

5. Conclusion

We are shifting from an era where products were tagged and tracked manually, occasionally, for discrete, siloed stages during the life cycle. In this new era products are being connected to the cloud continuously, throughout manufacturing, distribution, retail, consumption and recycling. This opens up much greater utility, opportunities for savings and increased value at each stage. These benefits will only accrue if the interests of each party at every stage are balanced equitably, if data is shared appropriately and privacy is respected. This paper has laid out some of the principles with which to do that. The winners in this new era will be those that apply these principles artfully and seize the day.

[13] https://www2.deloitte.com/global/en/pages/consumer-business/articles/consumer-data-give-and-take.html

Authors

Jesper Mathias Nielsen, Deloitte

Manager, NextGen

jesnielsen@deloitte.dk

Jonas Sveistrup Søgaard, Deloitte

Industrial PhD, NextGen

jsveistrup@deloitte.dk

Rasmus Winther Mølbjerg, Deloitte

Director, Nordic Emerging Technologies Lead

rmoelbjerg@deloitte.dk

Anne Kathrine Wennergren Holm, Deloitte

Partner, Responsible Innovation and Technology

anneriksen@deloitte.dk

Robert Schmid, Deloitte

Managing Director, Chief Futurist

roschmid@deloitte.com

Stephen Statler, Wiliot

SVP Marketing and Business Development

steve.statler@wiliot.com