Business Horizons (2023) 66, 493—504

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.journals.elsevier.com/business-horizons

Data-driven business and data privacy: Challenges and measures for product-based companies

Fabian Schäfer [a], Heiko Gebauer [a,b,c,*], Christoph Gröger [d], Oliver Gassmann [a], Felix Wortmann [a]

[a] *Institute of Technology Management, University of St. Gallen, Dufourstrasse 40a, 9000 St. Gallen, Switzerland*
[b] *Fraunhofer-Zentrum für Internationales Management & Wissensökonomie IMW, Neumarkt 9, 04109 Leipzig, Germany*
[c] *Department of Management & Engineering, Linköping University, 581 83 Linköping, Sweden*
[d] *IoT & Digitalization Architecture, Robert Bosch GmbH, Borsigstrasse 4, 70442 Stuttgart, Germany*

KEYWORDS
Data-driven business;
Data privacy;
Digital services;
Risk management;
Data sharing;
Privacy principles

Abstract To leverage the opportunities provided by the Internet of Things (IoT), product-based companies are exploring new data-driven business opportunities. They may miss these same opportunities, however, owing to data-privacy challenges. These challenges start with the customers of product-based companies, extend to the wider business ecosystem, and continue with the companies themselves. This article identifies 12 data-privacy challenges and introduces 12 measures to address them. These include intuitive recommendations, such as enabling cross-product consent collection, as well as less intuitive measures, such as fostering a can-do attitude in legal units, closing the gap between legal and business initiatives, or implementing a clear process for well-reasoned risk-taking. The following four principles were found to support companies in implementing these measures: (1) letting privacy and data-driven business go hand in hand, (2) putting customers first and turning their privacy preferences into opportunities, (3) aligning risk-management activities with the process of digital service development, and (4) using technology to professionalize legal processes.

* Corresponding author
E-mail addresses: fabian.schaefer@unisg.ch (F. Schäfer), heiko.gebauer@unisg.ch (H. Gebauer), christoph.groeger@de.bosch.com (C. Gröger), oliver.gassmann@unisg.ch (O. Gassmann), felix.wortmann@unisg.ch (F. Wortmann)

https://doi.org/10.1016/j.bushor.2022.10.002

1. Leveraging data from smart, connected products for data-driven business

The Internet of Things (IoT) encourages product-based companies to make products that are smart and connected. Companies are now equipping their physical products with sensors, data storage possibilities, connectivity components, microprocessors, and software features. Smart, connected products allow companies to gain access to product usage data (Porter & Heppelmann, 2014). Typical examples of smart, connected products now go beyond smartphones and extend to vehicles, home devices, and other machines. Such smart, connected products have given rise to new touchpoints with product users that companies could not have previously reached.

For example, car manufacturers are now able to access data about car usage even as far as recognizing whether drivers and passengers turn on the seat heating systems in winter. As a result, car manufacturers not only receive data about the car's condition but also personal data about drivers and passengers. Similarly, smart home system providers can access data about personal energy consumption, and machine manufacturers gain access to both machine and operator performance information.

Accordingly, product-based companies are trying to explore data-driven business opportunities, seeking to identify, create, and capture more value from data and data analytics. In the process, companies are even rethinking their organizational boundaries and starting to embrace data-sharing practices with partners in their surrounding business ecosystems (Chen et al., 2011; Ransbotham & Kiron, 2017). While leveraging data from smart, connected products resonates with the idea of data being a key resource for achieving competitive advantages (Bilgeri et al., 2019; Hartmann et al., 2016), data privacy is also becoming a key obstacle for product-based companies.

One statute driving data-privacy concerns is the European General Data Protection Regulation (GDPR). It is considered the world's strictest data-protection regulation and has become a global blueprint for data-privacy regulations in other regions (Akhlaghpour et al., 2021; Godinho de Matos & Adjerid, 2022; Lee, 2021; Mazurek & Małagocka, 2019). This regulation protects the aforementioned personal data on car usage, energy consumption, and machine operation. Since such data-privacy regulation can constrain collection of data from smart, connected products for data-driven businesses, recent research has called for further investigation into data privacy (Carrera-Rivera et al., 2022; Cichy et al., 2021). In response to this call, our research focuses on data-privacy challenges and corresponding measures for product-based companies.

Section 2 of this article highlights data privacy as being both a threat and an opportunity for data-driven businesses. Section 3 elaborates on challenges that companies face when dealing with this threat and exploring this opportunity. Section 3 also introduces measures to address these challenges. The fourth and final section explains four principles for implementing these measures successfully.

2. Privacy as a threat and opportunity for data-driven businesses

Legal and regulatory requirements as well as customers' privacy preferences can limit data-driven businesses. When the GDPR came into effect in 2018, it started protecting any information given about an identified or identifiable natural person (e.g., a person's name, ID, or location) to ensure customer privacy (GDPR, 2018). Customer privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7).

Since customers are very attentive to privacy issues (Cichy et al., 2021; Salesforce Research, 2022), the fact that companies may be held responsible for activities violating their customers' privacy, including the processing of data for purposes for which companies have not received consent by their customers, constitutes a threat. If companies are not compliant with the GDPR (2018), they may be liable to pay an administrative fine of 4% of company revenue—or a minimum of €20 million. The likelihood of this happening increases as companies share more and more data with partners within the business ecosystem. Companies are increasingly losing control over data, making it more likely that either they or their partners will violate customer privacy (Chanson et al., 2019). Such possible threats cause legal uncertainties, which in turn lead to companies refraining from innovation activities on the grounds of data privacy (Bitkom, 2020).

Data privacy can constitute not only a threat but also an opportunity for achieving a competitive advantage (Goldfarb & Tucker, 2013). Car manufacturer Daimler (2019, p. 5) stated:

> People are worried that their data could be misused. We don't want to play down these fears—on the contrary, we want to build trust.... Sustainable innovations are the only way we can build trust and have lasting success.

If companies gain trust from customers, they can turn data-driven innovation and data privacy into competitive advantages.

However, research remains unclear as to how such challenges and the measures associated can turn data privacy from a threat into a business opportunity within the context of smart, connected products (Gerlach et al., 2018). To close this research gap, we investigated in two steps how companies turn data from smart, connected products into data-driven business opportunities. In the first step, we conducted five in-depth case studies together with two smart home providers (Future Tech, SmartHub), a power tool provider (Timco), a mobility provider (Power Wheel), and an optical systems and optoelectronics company (OpTech). We chose these case studies owing to their rich empirical context for collecting personal data through smart, connected products. They are also interesting since they embody typical legal hurdles between headquarters, business divisions, and local sales organizations. We collected data for these case studies through interviews and workshops with managers from relevant functions (e.g., business, legal, technology, software). To deepen the insights, further interviews were conducted with companies that offer solutions in the fields of legal technology (LawTech Partners), consent management (ConTech) and privacy management (Privatech). The interviews and workshops resulted in about 20 hours of recorded and transcribed conversation time. The five case studies were analyzed by means of both within-case and cross-case analysis.

In the second step, we investigated successful practices for data-driven businesses. We asked executives from the five case studies to point out industry leaders (Apple, Daimler, Facebook, Google, Microsoft, Tesla). We collected secondary data—including annual reports, company publications, and presentations—about these leaders. The analysis of this data supported the findings emerging from the first study and was consistent with the existing literature (see Figure 1).

3. How companies compliantly leverage data-processing opportunities

Our two studies on the five in-depth cases and six successful practice companies revealed 12 common key challenges and measures for leveraging data from smart, connected products for data-driven businesses. These 12 challenges cover three perspectives: user-, ecosystem-, and organization-centered (see Figure 2). The perspectives cover the user, the ecosystem partners, and the product-based company itself as key actors involved in the exchange of personal data and the creation of value through data-driven business models (Casadesus-Masanell & Hervas-Drane, 2020; Mazurek & Małagocka, 2019).

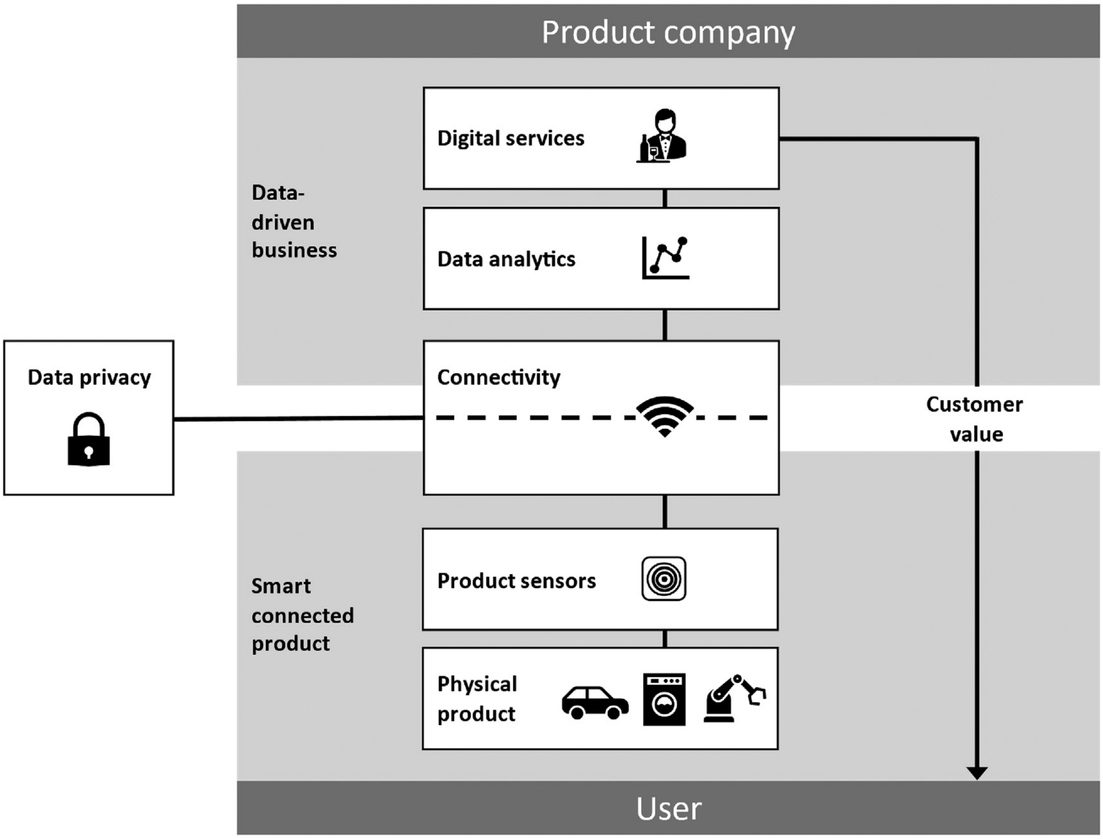
3.1. User-centered perspective

Data-driven businesses require a smooth exchange of data between product users and product providers. To convince product users to exchange their own data, it is insufficient simply to propose value to them in terms of receiving a digital service in return for the data. To build trust, companies need to take a user-centered perspective. Building trust among customers and users is a prerequisite for data exchange between those users and the product providers (Mazurek & Małagocka, 2019; Morey et al., 2015). Once customers trust the product providers, these companies can obtain legal consent from their users for the data exchange in alignment with the GDPR. Establishing such trust is far from easy. Clearly, users have usually already developed a certain level of trust in a company (Mazurek & Małagocka, 2019). Companies have, however, gained this trust specifically for their high-quality and reliable products and not as yet for their digital touchpoints. As a result, there are four challenges to overcome from a user-centered perspective (see Figure 2).

3.1.1. a. Challenge 1: Determining the appropriate strength of self-imposed privacy principles

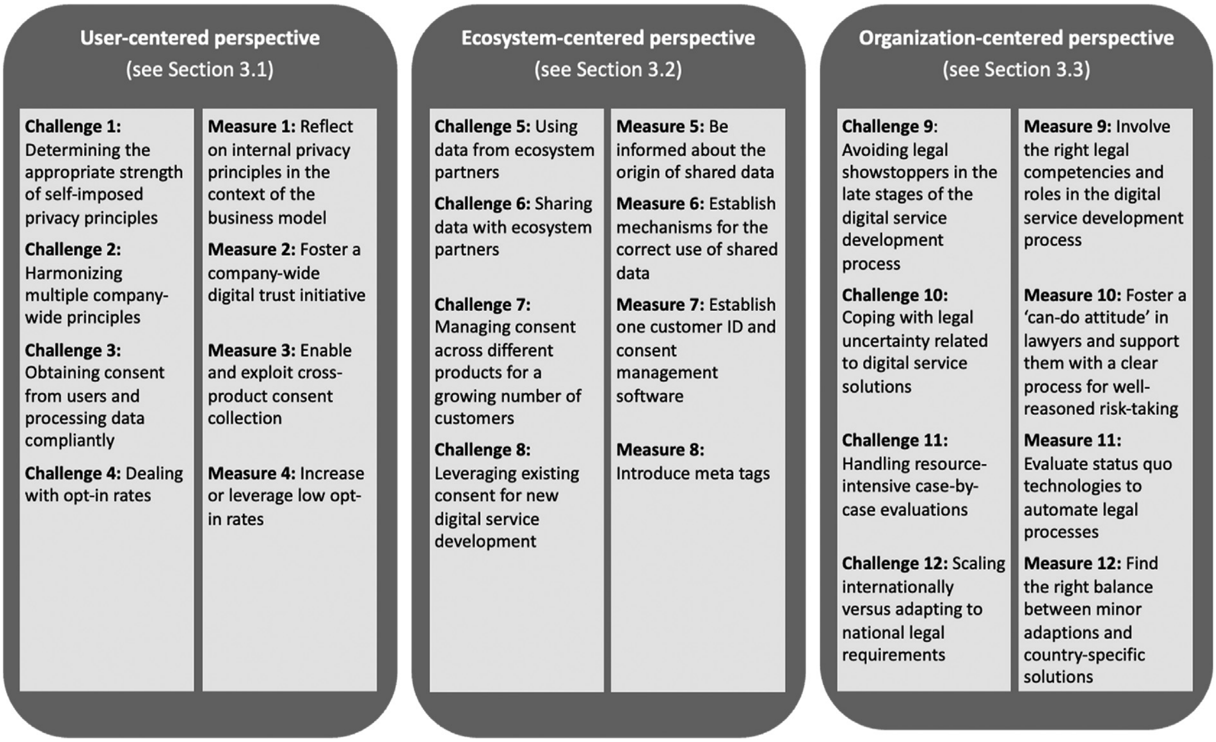
By communicating privacy principles to their customers, companies highlight their own commitment to trust (Mazurek & Małagocka, 2019; Morey et al., 2015). Privacy principles are a "set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems" (International Organization

Figure 1. Data privacy as an obstacle for data-driven business.



Source: Adapted from Fleisch et al. (2014)

Figure 2. Key privacy challenges and measures in the realm of data-driven business



User-centered perspective (see Section 3.1)

Challenge 1: Determining the appropriate strength of self-imposed privacy principles	**Measure 1:** Reflect on internal privacy principles in the context of the business model
Challenge 2: Harmonizing multiple company-wide principles	**Measure 2:** Foster a company-wide digital trust initiative
Challenge 3: Obtaining consent from users and processing data compliantly	**Measure 3:** Enable and exploit cross-product consent collection
Challenge 4: Dealing with opt-in rates	**Measure 4:** Increase or leverage low opt-in rates

Ecosystem-centered perspective (see Section 3.2)

Challenge 5: Using data from ecosystem partners	**Measure 5:** Be informed about the origin of shared data
Challenge 6: Sharing data with ecosystem partners	**Measure 6:** Establish mechanisms for the correct use of shared data
Challenge 7: Managing consent across different products for a growing number of customers	**Measure 7:** Establish one customer ID and consent management software
Challenge 8: Leveraging existing consent for new digital service development	**Measure 8:** Introduce meta tags

Organization-centered perspective (see Section 3.3)

Challenge 9: Avoiding legal showstoppers in the late stages of the digital service development process	**Measure 9:** Involve the right legal competencies and roles in the digital service development process
Challenge 10: Coping with legal uncertainty related to digital service solutions	**Measure 10:** Foster a 'can-do attitude' in lawyers and support them with a clear process for well-reasoned risk-taking
Challenge 11: Handling resource-intensive case-by-case evaluations	**Measure 11:** Evaluate status quo technologies to automate legal processes
Challenge 12: Scaling internationally versus adapting to national legal requirements	**Measure 12:** Find the right balance between minor adaptions and country-specific solutions

for Standardization, 2011, p. 3). But few companies already comply with the GDPR or have established public privacy principles (Jiang et al., 2020). When designing privacy principles, companies need to balance the strictness required to avoid privacy disasters with the leeway needed for the development of digital services (Culnan, 2019; Spiekermann, 2012). Our comparison of successful practice companies with the experience of product-based companies suggests that product-based companies still seem not to use privacy principles strategically. One interviewee stated:

> [Microsoft says] right from the start [of a collaboration], 'Well, the data belongs to you.' [...] In contrast to Google, which wants to keep everything and continue to use it for itself. [OpTech] does not have [privacy principles] yet in that way [...] but it is a way forward at some point, which must be derived from our strategy. (Head of strategic corporate development, OpTech)

3.1.1. b. Measure 1: Reflect on internal privacy principles in the context of the business model

To design privacy principles strategically, companies need to reflect on their principles beforehand to avoid self-imposed restrictions that weaken their own business. Apple (2021), for example, introduced the concept of "on-device processing" and promised that it would process its customers' data, if technically possible, only on the customers' devices, having no interest in selling customer data to advertisers. This principle builds strongly on the strategic direction Apple has been following. In 2015, Tim Cook (CEO) explained: "Our business model is very straightforward: [...] We don't 'monetize' the information you store on your iPhone [...] Our software and services are designed to make our devices better" (Morey et al., 2015, p. 104). Apple's privacy principle goes hand in hand with its business model. Like other product-based companies, Apple also owns the hardware behind the digital services it provides to its customers. Its business model differs, however, from that of Google, where personal data are key for value creation through personalized advertisements (Casadesus-Masanell & Hervas-Drane, 2015).

3.1.2. a. Challenge 2: Harmonizing multiple company-wide principles

Artificial intelligence (AI), as a key to data processing and analytics, contributes to the convergence of privacy and security (Burt, 2019). In addition to privacy principles, companies can also establish AI principles (Smit et al., 2020). With the boundaries between privacy and security being blurred and the variety of principles increasing, companies should work to present a uniform appearance to the outside world regarding their use of data.

3.1.2. b. Measure 2: Foster a company-wide digital trust initiative

Digital trust can be used as an umbrella term for behavioral and cultural guidelines relating to data privacy, security and AI ethics. Furthermore, the term itself refers to a company's actual goal, which is establishing trust with its users. To engender digital trust, managers need to set up company-wide digital initiatives that join and harmonize existing principles encompassing their internal organization (Abraham et al., 2019; Kluiters et al., 2022). For instance, Daimler (2021) addressed the topics of privacy, security, and AI ethics in its data-compliance management system initiative and explicitly relates its AI use to its privacy principles, stating: "Our guiding principles for data have thus been supplemented by our Principles for Artificial Intelligence. [...] Together with the guiding principles for data, they serve as an important foundation for our digital responsibility."

3.1.3. a. Challenge 3: Obtaining consent from users and processing data compliantly

Companies must ensure that personal data are used only for well-defined purposes for which user consent is provided (GDPR, 2018). The data processed for each operation should be limited to the extent required to achieve that purpose, and companies need to justify processing a user action timestamp to execute a certain function. As one interviewee stated: "In smart home environments, timestamps are categorized as personal data as they give companies insights into usage behavior, allowing to predict user actions" (data protection specialist, SmartHub).

3.1.3. b. Measure 3: Enable and exploit cross-product consent collection

The collection of data through smart, connected products allows companies to gather consent through websites and smartphone apps, where users usually need to tick a box after having read a statement. In addition, some companies collect consent through the interfaces of multimedia systems in vehicles. One workshop participant observed:

> This is not so easy, because the customer must be able to give the consent [...] [and] to revoke it. [...] Creating these conditions is perhaps even easier with a pure app [...] [on] a motorcycle, it becomes a bit more difficult. (Digital business analyst, Power Wheel)

But this can also present an opportunity to gain higher consent rates, as another interviewee pointed out: "collecting consent in the car may lead to higher consent rates, as drivers prioritize driving in that context more than privacy" (entrepreneur in residence, ConTech).

3.1.4. a. Challenge 4: Dealing with opt-in rates

Users' behavior when asked for consent depends heavily on how the consent form provided is designed (Utz et al., 2019). For example, specific features such as the color of the individual elements of the form and their position on the screen can have a decisive influence on the opt-in rate. Furthermore, companies that fail to build trust, whether owing to absent privacy principles or past privacy scandals, find it difficult to obtain high opt-in rates for their digital services.

3.1.4. b. Measure 4: Increase or leverage low opt-in rates

A/B testing allows companies to show different consent forms to equal-size user groups for a predefined period to determine which consent form configuration can help to increase the opt-in rate. If companies struggle to increase opt-in rates, they can utilize anonymized data to enable the processing of data for which companies have not received consent. The GDPR (2018) defines anonymous data as data that are rendered anonymous in such a way that the data subject is not, or is no longer, identifiable. One interviewee indicated: "The analyses of purely-based anonymized data can lead to misleading findings" (data protection specialist, SmartHub). To address this, SmartHub created a data lake combining both anonymized and nonanonymized data depending on the user consent available. Upon analyzing anonymized data from oven sales in a specific market, the company's data scientists recognized an increased tendency to use a particular program for baking buns. One conclusion possible was that this function was very popular and would provide an interesting starting point for further innovation. To validate this insight, however, they performed a counter test with a subset of nonanonymized data and thus found out that only a small number of very specific customers (bakeries) frequently used the baking program in question. The detection of this misleading finding was only made possible through analyzing nonanonymized data referring to a particular device ID. In conclusion, even if not every user gives consent, anonymized user data are helpful in recognizing tendencies, and the proportion of data for which consent is given can serve as a sample for the validation of those tendencies. It is worth noting that this measure also serves to mitigate risks such as data breaches, as the proportion of personal data at risk is much lower.

3.2. Ecosystem-centered perspective

Companies should also take an ecosystem-centered perspective. This, however, means companies have to deal with privacy challenges when sharing data with other companies in the ecosystem. Establishing an appropriate and effective consent-management infrastructure is the backbone for effective data sharing in ecosystems. Companies must ensure that they share data compliantly and in line with their users' privacy preferences. Customer privacy preferences are heterogeneous and lead to individual consent decisions for each ecosystem partner (Cichy et al., 2021). To ensure reliable user consent across users and their products as well as with their ecosystem partners, companies need to face the following four challenges and apply corresponding measures (see Figure 2).

3.2.1. a. Challenge 5: Using data from ecosystem partners

Some companies may find themselves unable to source sufficient personal data with their own products, as their current products may not yet have the capability needed, and product development cycles require several years. Such personal data are of particular interest to companies that want to get to know their users better. For example, data about driving behavior can be derived through location tracking and tabulating driving hours. One interviewee stated, "We still need the smartphone [...] so there is no connection to the bike [...] But that simply has to do with the fact that the product was introduced 2—3 years ago" (digital business analyst, Power Wheel). To avoid shortfalls of data, companies need to build capabilities to access and share data with ecosystem partners. They are dependent on the privacy standards of the partner that initially collects the data with their smart, connected products. Accordingly, they must clarify whether user consent was received for data collection and sharing.

3.2.1. b. Measure 5: Be informed about the origin of shared data

Publicly communicated privacy principles can shed light on the practices of ecosystem partners. Additionally, companies can map their data supply chains using privacy-management software. One interviewee stated with regard to providing vendors with risk assessments for databases: ″We work with questionnaires, certain checklists to check the compliance [of a vendor]” (senior solutions engineer, Privatech). Such risk assessments include industry-standard questionnaires designed to check compliance with GDPR requirements and are a means of increasing trust in partners.

3.2.2. a. Challenge 6: Sharing data with ecosystem partners

Companies often run multiple business units, which act as separate legal entities. Legally independent business units are not subject to any group privilege with regard to data sharing and should be treated like third-party companies, which must secure user consent before sharing data between business units. This situation has prompted observations that data often remain in silos (Ransbotham & Kiron, 2017).

Another scenario is the sharing of data across company boundaries with partners. In particular, the success of advertisement-based business models depends on a company's data-sharing capability. For instance, while Facebook's business model requires the sharing of data between partners, the Cambridge Analytica case showed how it was possible for personal data from 87 million users to be misused by third parties, even though the underlying contractual framework should not have allowed for such behavior (Kozlowska, 2018). Hence, having shared its data, Facebook lost control of the data. Through the increasing connectivity of their products and the growing interconnectedness of partners in data ecosystems, product-based companies increasingly collect and share highly sensitive information (Cichy et al., 2021). The investigated companies are quite careful with data sharing, as one interviewee stated: ″Data security for customers is our top priority, we must expect or demand the same from those with whom we work” (manager for digital strategy and innovation, Timco).

3.2.2. b. Measure 6: Establish mechanisms for the correct use of shared data

When data are shared within companies between multiple legally independent business units, consent must be managed across them. Thus, companies have to roll out consent-management tools that allow business units to share data and manage the associated consent together. In terms of external data sharing, the aforementioned vendor assessments (Measure 5) also support companies in assessing the risks of sharing data with partners.

3.2.3. a. Challenge 7: Managing consent across different products for a growing number of customers

Faster product-release cycles, particularly for software-based applications, make it increasingly difficult for companies to use their existing tools (e.g., Excel or SharePoint lists) for consent management. Although these tools may have been sufficient for managing customer data for traditional hardware-based businesses, they cannot handle the increasing complexity generated by the growing number of customers for those large-scale digital services distributed across several smart, connected products and for which data are shared with ecosystem partners. Furthermore, digital services usually require software updates and demand consent from users. Companies have to document who has agreed to what and when they did so.

3.2.3. b. Measure 7: Establish one customer ID and consent management software

To manage the consent of a single user, companies need to clearly identify the customer. A customer may have more than one touchpoint with a company, especially if a company offers a broad range of smart, connected products. A single customer ID is the key for transparent consent management. To incentivize its customers to stick to this single customer ID, OpTech introduced a digital attendant that helps the company accompany its customers through the lifecycles of their purchased products. Moreover, companies should ensure the traceability of customers' consent. Consent-management software can trace the latest version of this consent across different products (e.g., smart-home devices, connected cars, smartphone applications).

3.2.4. a. Challenge 8: Leveraging existing consent for new digital service development

A new service can provide features for novel purposes, but it can also process data for the same purposes for which a company has already received consent. Accordingly, having once received consent and being able to trace it enables companies to make use of it for new digital services.

3.2.4. b. Measure 8: Introduce meta tags

To check users' consent for a certain purpose, companies can break down consent statements into meta tags. As one interviewee explained:

> A company has the agreement of the customer that they may send a message when [...] the dishwasher salt is empty. This is a purpose. For that, I am allowed to process data. Now, instead of telling the user [...] 'Your salt is empty', you want to tell them 'buy the salt of [the brand] Henkel'. [...] [This] would require that the user has also agreed to a marketing communication. [...] ['Status messages about my device' and 'promotional messages'] are the meta tags. (Data protection specialist, SmartHub)

While meta tags are vital for consent management across company boundaries, companies must be aware that a broad interpretation of meta tags may defeat the actual purpose of data processing. Therefore, they need to balance the specificity required by meta tags with sufficient abstraction for the further use of data.

3.3. Organization-centered perspective

Companies should also take an organization-centered perspective to turn data privacy into a competitive advantage. But many companies' legal apparatuses are often involved too late in the exploration of new data-driven business opportunities, and many legal experts tend toward a counterproductive mindset for turning data into business opportunities. Companies need to bridge the gap between legal and business initiatives. Furthermore, they should determine how they can further develop their legal apparatuses and increase their efficiency. The organization-centered perspective is the final perspective to be applied, as every company has individual users and ecosystems with their own requirements.

From an organization-centered perspective, the challenge is how to enable a company to develop a digital service that is consistent with internal privacy values and external privacy regulations. To achieve this, it is not enough for new roles to be defined and those involved to be trained. The organization needs to create the conditions that enable different ways of thinking and behaving. This means that the organization must learn both how to bring new, data-driven business opportunities to life and how to bridge the gap between legal and business initiatives (see Figure 2).

3.3.1. a. Challenge 9: Avoiding legal showstoppers in the late stages of the digital service development process

Business developers often ask for legal support early during the development of digital services, when concepts are being designed, while legal experts prefer a clear concept for a service before they can conduct a legal assessment. Often, though, the requested concept is not available at an early stage, as one interviewee explained:

> You can't go to our legal department today and ask, 'what would we actually have to do to be allowed to work with telemetry data in a technically clean way?' Then you don't get an answer. The answer is, rather, 'yes, tell us exactly what you would like to do with which data in this case' [...] The strategic handling of data protection is not to be found in the legal department. (Digital business analyst, Power Wheel)

Early support allows a business to consider key legal privacy requirements from the beginning, while late legal assessments may lead to showstoppers after concepts have been finalized.

3.3.1. b. Measure 9: Involve the right legal competencies and roles in the digital service development process

Although companies are used to checklists and blueprints for legal assessments of hardware products, they need to approach legal questions regarding digital services differently. Such assessments require knowledge of privacy laws: "It is not possible to bring employees up to the level of being the data protection expert, [but they] should have an understanding of the basic mechanisms" (digital business analyst, Power Wheel). In addition, companies can implement completely new procedures for collaborating with corporate legal departments in the development of digital services:

> At some point, they call in the legal department and then at the end they only have the desire to get the approval from data protection. But this [...] may have made sense 10—15 years ago [...] [Today] you have to think about this data protection driver [in the

> development] of the whole business model from the very beginning. (Data protection lawyer, Future Tech)

To ensure that the right legal experts are involved from the start, the development process should trigger their involvement. But one workshop participant pointed out that development teams may not be able to clearly determine whether personal data will be collected or whether data-protection experts need to be involved, saying, "Even when triggered, the right people are missing to say that data protection is relevant here, because many people simply check off 'We don't have any personal data' without thinking about the product's scope" (data protection lawyer, Future Tech).

To solve this issue, the companies we examined argued that a single point of contact for legal topics is beneficial. This single contact point should involve the right people to answer the questions at the respective development stage. As a case in point, Daimler (2021) developed a technical compliance-management system that offers systematic legal consulting during the development process via a single point of contact.

3.3.2. a. Challenge 10: Coping with legal uncertainty related to digital service solutions

As digital services for smart, connected products present new legal issues, legal experts must conduct their assessments case by case; in contrast to the hardware business, blueprints and checklists do not exist in this area yet. This leads to uncertainty, as one interviewee explained:

> Data stored with the chassis number is personal data; yes, it is ultimately a doctrine that is currently spreading. Only we simply do not yet have any judicial decisions on this case [...] [So] you are simply caught up in an absolute uncertainty. (Digital business analyst, Power Wheel)

This uncertainty provides for a great deal of legal leeway. If companies shy away from applying this leeway because they wish to mitigate legal risks (i.e., administrative fines), they may end up applying data-privacy regulations to scenarios for which they were neither intended nor designed by the legislator and thereby put their business opportunities at risk (Batura & Peeters, 2021).

3.3.2. b. Measure 10: Foster a can-do attitude in lawyers and support them with a clear process for well-reasoned risk-taking

To resolve this issue, a paradigm shift in the mindset of lawyers is required, meaning that data protection will no longer be seen in its gatekeeper function but as a business driver. Lawyers need to navigate business developers through the legal solution space and synchronize legal with business solutions. They need to perceive their duties as consulting activities and explain how something can be adapted within legal parameters:

> You must have people in the legal department [...] who come out of the 'can-do attitude' and [...] say 'we want to find a way to do this' and not [...] 'I'll check if something is 100% waterproof and intervene if it's not'. (Head of strategic corporate development, OpTech)

Data protection was once a technical issue; today, it is mainly a legal issue. Accordingly, a company's data protection officer's qualifications provide an important basis for this shift in mindsets. The data-protection lawyer from Future Tech explains this fundamental problem as follows:

> On the legal level, it fails because of technical understanding and the time to be able to provide technical advice. [...] And on the technical side, it fails because of the legal skills needed to incorporate what has been technically devised into the legal norms.

Companies need to make sure that they recruit employees with appropriate skills for this position.

In addition, companies have to answer two fundamental questions: Which risks are the company willing to accept? And who is liable for these risks? Hence, companies need a clear process for risk-taking that calculates the risk for digital service design decisions and aligns the decisions with companies' appetites for risk.

The assessment of the risk in an individual case should focus on risk-increasing factors. Business process models and intercompany data-flow models can help to identify these factors. But in regard to data privacy, the identified risks may not be fully mitigable, and the potential impacts of these risks can make executives reluctant to accept them. As one interviewee explains: "Tell a manager he should take the risk for a fine of 100 million. The answer is clear. This risk is not taken" (Data protection lawyer, Future Tech).

The impact of these decisions makes them strategic management decisions. Managers can pursue two strategies: either to push it on the market and adjust or to actively involve the legislator. According to one interviewee, the first strategy is pursued by companies willing to take risks: "American companies, especially Facebook, Google, Tesla [...] take every risk and try to solve it afterwards [...] [and] look at the business advantage. Namely, ‘we can now develop something that will make us the global market leader’” (Data protection lawyer, Future Tech).

The extent to which this strategy is feasible differs according to a country’s or region’s risk-taking attitude. For instance, the first of the above-mentioned strategies would be unacceptable in many traditional European companies. But those companies may accept a lively exchange with the regulatory authorities regarding untested practices for which there are no legal precedents.

3.3.3. a. Challenge 11: Handling resource-intensive, case-by-case evaluations

Novel legal cases have ensued from both the increase in digital service initiatives and the introduction of new worldwide regulations. Companies are eager to minimize legal risk as they enter into contracts with many partners, within ecosystems where data are shared for different purposes. As data-driven business models and their reasons for sharing and processing may vary, legal issues must be assessed case by case. This increases legal costs and the amount of resources required.

3.3.3. b. Measure 11: Evaluate status quo technologies to automate legal processes

Legal cases and contracts resulting from negotiations need to be stored centrally, thus enabling knowledge sharing between lawyers. Referring to a database of such cases, one interviewee explained that legal technology can help to automate case-by-case assessments by applying natural-language processing and identifying patterns in cases over a longer period: "Amazon tells you that users who bought this item also bought certain other items. In legal tech, an intelligent recommender system would tell lawyers how other lawyers have solved a similar case and which other questions they addressed” (executive director, LawTech Partners). Based on data from contract negotiations, legal technology can support lawyers in their negotiations with potential suppliers and partners by identifying similar contract situations and the negotiation strategies applied.

3.3.4. a. Challenge 12: Scaling internationally versus adapting to national legal requirements

The companies we examined already distribute their digital services globally. Processing data for their service offerings outside of Europe requires them to meet the local privacy requirements for data processing. In addition to the GDPR, stringent regulations are being introduced globally, including the California Consumer Privacy Act (CCPA), the Brazilian General Data Protection Law (LGPD), and the Indian Data Protection Bill. The resulting variations in local legal requirements, however, hamper the scalability of digital services (Wentrup & Ström, 2019).

For their hardware-based businesses, the companies we examined have processes with which to adapt their hardware products to local requirements. In the case of Timco, its country-specific sales companies are responsible for meeting country-specific regulations. But in regard to the digital applications for the company’s smart-home products, Timco’s data strategist argued: "It makes no sense when every country has its own app and manages its own back-end. We have to think of a solution for the whole world.”

3.3.4. b. Measure 12: Find the right balance between minor adaptations and country-specific solutions

Some companies may choose to ensure compliance with an existing strict privacy law before moving on to compliance with other laws or in other regions. For example, as a first step, compliance with the GDPR may also be beneficial in achieving compliance in non European markets:

> We had the case where we said we are doing this first for the EU, [...] and then we are going into our, I call it problem markets, from a legal point of view. That is the USA; that is China; that is Russia. [...] And once we have overcome the major pitfalls, there is a good chance that we will find a solution in other countries as well. (Data strategist, Timco)

But the head of strategic corporate development at OpTech recognized that for OpTech’s digital services to meet the legal requirements in some countries, a completely new solution is required, saying, "There must be two solutions. One for China and one for the rest of the world.”

To find the right balance between the smallest common denominator and the scope of individual solutions, companies must be aware of emerging regulations. If companies want to scale their digital services globally, they either need to comply with regulations that minimize the legal risk in those global markets or must avoid features that require adaptation.

4. Implementation principles

In implementing these 12 measures for overcoming the aforementioned challenges, companies should adopt the following principles.

4.1. Privacy and data-driven business must go hand in hand

Privacy is not simply a topic that has to be addressed to comply with privacy regulations; Companies should learn from successful businesses (e.g., Apple, Google, Facebook) how to communicate privacy principles. These privacy principles should be an integral part of any marketing campaign. In fact, companies need to address this topic to build customer trust, to obtain access to customer data, to deliver new digital services, and ultimately, to increase their profitability.

4.2. Put customers first and turn their privacy preferences into opportunities

Before companies can define their privacy principles and go on to create digital services, they have to ensure that they sufficiently understand their customers' privacy preferences. During our research, we observed that companies are often unaware of these preferences, having focused their privacy efforts too narrowly on compliance requirements and regulations.

4.3. Align risk-management activities with the process of digital service development

Uncertainty and legal risks form an integral part of digital service development. Executives need to ensure that they establish risk-management systems that include roles that identify these risks, as well as establish procedures for efficient risk assessment and decision-making. In the development process, data-protection officers with technical and legal knowledge can help to identify risks early on and can provide assessments to enable managers to make informed decisions.

4.4. Professionalize and improve legal processes through technology

While the use of AI to automate legal processes is still a long way off, new software tools more appropriate to the complexities of consent management will increase the efficiency of legal tasks and prevent some common mistakes. These tools will require investment, so decision-makers in manufacturing companies must seriously consider these recommendations and begin by doing some basic groundwork.

To conclude, even if these insights regarding the challenges, measures, and principles of data-driven business and data privacy for product-based companies are not meant to be exhaustive, they will be helpful for both academics and practitioners as they grapple with today's evolving markets and regulatory environments. They should also provide a valuable starting point for companies eager to begin laying the groundwork to meet future regulations.

References

Abraham, C., Sims, R. R., Daultrey, S., Buff, A., & Fealey, A. (2019). How digital trust drives culture change. *MIT Sloan Management Review, 60*(3), 1–8.

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., & Hynd, A. (2021). Learning from enforcement cases to manage GDPR risks. *MIS Quarterly Executive, 20*(3), 199–218.

Apple. (2021, April). *A day in the life of your data*. Available at https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

Batura, O., & Peeters, R. (2021, July). *European Union data challenge*. Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662939/IPOL_BRI(2021)662939_EN.pdf

Bilgeri, D., Gebauer, H., Fleisch, E., & Wortmann, F. (2019). Driving process innovation with IoT field data. *MIS Quarterly Executive, 18*(3), 191–207.

Bitkom. (2020, September 29). *One in two companies refrains from innovations for privacy reasons*. Available at https://www.bitkom.org/Presse/Presseinformation/One-in-two-companies-refrains-from-innovations-for-privacy-reasons

Burt, A. (2019, January 3). Privacy and cybersecurity are converging. Here's why that matters for people and for companies. *Harvard Business Review*. Available at https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

Carrera-Rivera, A., Larrinaga, F., & Lasa, G. (2022). Context-awareness for the design of smart-product service systems: Literature review. *Computers in Industry, 142*, 103730.

Casadesus-Masanell, R., & Hervas-Drane, A. (2015). Competing with privacy. *Management Science, 61*(1), 229–246.

Casadesus-Masanell, R., & Hervas-Drane, A. (2020). Strategies for managing the privacy landscape. *Long Range Planning, 53*(4), 101949.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20*(9), 1274–1309.

Chen, Y., Kreulen, J., Campbell, M., & Abrams, C. (2011). Analytics ecosystem transformation: A force for business model innovation. In *Proceedings of the 2011 Annual SRII Global Conference* (pp. 11–20). Piscataway, NJ: IEEE.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the Internet of Things: Mixed method evidence from connected cars. *MIS Quarterly, 45*(4), 1863–1891.

Culnan, M. J. (2019). Policy to avoid a privacy disaster. *Journal of the Association for Information Systems, 20*(6), 848–856.

Daimler. (2021). *Responsible use of data — Data compliance management at Daimler*. Stuttgart, Germany: Daimler.

Daimler. (2019, January 28). *New digital business models and data protection — A contradiction in terms?* Stuttgart, Germany: Daimler.

Fleisch, E., Weinberger, M., & Wortmann, F. (2014). *Business models and the Internet of Things* [White Paper]. Zurich, Switzerland: Bosch IoT Lab.

GDPR. (2018). *General data protection regulation*. Available at https://gdpr.eu/tag/gdpr/

Gerlach, J. P., Eling, N., Wessels, N., & Buxmann, P. (2018). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal, 29*(2), 548–575.

Godinho de Matos, M., & Adjerid, I. (2022). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Science, 68*(5), 3330–3378.

Goldfarb, A., & Tucker, C. (2013). Why managing consumer privacy can be an opportunity. *MIT Sloan Management Review, 54*(3), 10–12.

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data — A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations and Production Management, 36*(10), 1382–1406.

International Organization for Standardization. (2011). *Information technology — Security techniques — Privacy framework*. [ISO/IEC Standard No. 29100:2011]. Available at https://www.iso.org/standard/45123.html

Jiang, Z., Tolido, R., Jones, S., Hunt, G., Budor, I., Bartoli, E., van der Linden, P., Buvat, J., Theisler, J., Wortmann, A., Cherian, S., & Khemka, Y. (2020). *Championing data protection and privacy: A source of competitive advantage in the digital century*. Paris, France: Capgemini.

Kluiters, L., Srivastava, M., & Tyll, L. (2022). The impact of digital trust on firm value and governance: An empirical investigation of US firms. *Society and Business Review*. Available at https://doi.org/10.1108/SBR-07-2021-0119

Kozlowska, I. (2018, April 30). Facebook and data privacy in the age of Cambridge Analytica. *University of Washington*. Available at https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659–671.

Mazurek, G., & Małagocka, K. (2019). What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. *Business Horizons, 62*(6), 751–759.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*(5), 96–105.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64–88.

Ransbotham, S., & Kiron, D. (2017). Analytics as a source of business innovation. *MIT Sloan Management Review, 58*(3), 1–16.

Salesforce Research. (2022). *State of the connected customer* (5th ed.) Available at https://www.salesforce.com/eu/resources/research-reports/state-of-the-connected-customer/

Smit, K., Zoet, M., & van Meerten, J. (2020). A review of AI principles in practice. In *Proceedings of the Pacific Asia Conference on Information Systems* (pp. 198–211). Dubai, UAE: PACIS.

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM, 55*(7), 38–40.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990) New York, NY: ACM.

Wentrup, R., & Ström, P. (2019). Service markets: Digital business models and international expansion. In A. Aagaard (Ed.), *Digital business models: Driving transformation and innovation* (pp. 169–199). Cham, Switzerland: Palgrave Macmillan.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.