wejo | CtrlShift

THE GROWTH OF THE CONNECTED VEHICLE DATA MARKET – THE IMPLICATIONS OF PERSONAL DATA AND EMERGING US LEGISLATION

05

The importance of consumer trust and regulation to the connected car data market

05 | THE IMPORTANCE OF CONSUMER TRUST AND DATA REGULATION TO THE CONNECTED CAR DATA MARKET

In the fourth report in this series, we consider the key issue of consumer trust in the use of connected vehicle data and PII. As public awareness of issues around data security and privacy has grown, it is essential that data in the market is properly regulated. Accurate data is essential to the growth of the market, but if customer trust is not earned and maintained through the protection of personal data, the many benefits that the market presents will be significantly constrained.

Providers must build consumer and regulator confidence by being transparent about how data is collected and used, while proactively raising the benefits of data collection. Those involved in the market should lead by trust, using best practice to put the customer at the centre. They should strive to be at the forefront of developing legislation that supports the beneficial use of connected car data for all stakeholders, advocating self-regulation and always adhering to legislation.

Key Findings	Personal data and consumer trust are critical to the growth of the market for connected vehicle data. If trust is not earned and maintained by market participants, or if legislation fails to balance the need to protect privacy and ensure data security with the need to foster innovation and economic growth, then significant market opportunities and societal benefits could be materially constrained. There are wider risks where the operation of the market for vehicle data is impacted by issues and concerns with social networks' use of data and the regulatory response to failings in that market To mitigate these risks participants in the connected vehicle data market need to ensure they secure both consumer trust and the effective regulation of the use of data in the market. These include: ○ Stimulate consumer and regulator confidence: by encouraging transparency and raising proactively the profile of the connected car data market and the benefits it conveys. ○ Differentiation and leadership through trust: opportunity, to lead the market through trust – based on best practice and putting the individual at the centre - 'transparency', informed and practical consent, choice and education. ○ Positively influencing developing legislation to support the beneficial use of connected car data for all stakeholders, whilst ensuring the necessary data protections. There are a number of new data privacy acts being developed in US States as well as evolving understanding of the requirements of existing legislation such as GDPR in Europe and the unique characteristics and benefits of vehicle data need to be factored in to the design of legislation. ○ Self-regulation & Codes of Conduct: opportunity for OEMs and other market participants to build both consumer and regulatory trust through the advocacy and development of self-regulation ○ Actively promote the benefits of the connected car data market: stimulate consumer and regulator confidence by raising the positive profile of the connected car data market and the benefits it conveys

Connected car data is hugely valuable and it is vital that data is used responsibly. Vehicle manufacturers using sensors to collect the data, marketplaces that use it, firms that provide services build on it, and the individuals and companies using products powered by that data need to know that they are using ethically sourced information.

Important factors associated with PII, notably consumer trust and data privacy legislation and regulation are increasingly key issues in the development of the market. Furthermore, there is a significant risk that if consumer trust becomes undermined, and/or if PII legislation does not balance the need to protect privacy with the need to foster economic growth, the significant market opportunities detailed in Sections 2 and 3 could be materially constrained.

1.1. Consumer Trust

Consumer attitudes towards the use of personal data has been changing rapidly. For many years the rapidly expanding use of PII by organisations, fuelled by the explosive growth in consumers' online activity, was low profile and therefore little understood, or focused on by most consumers.

However, high profile mass data breaches e.g. Equifax and, in particular, the Cambridge Analytica debacle have turned the spotlight on personal data privacy and on the behaviour of social networks and mobile phone applications in particular. The increase in the profile of personal data risks undermining trust and consumer confidence in particular in companies and in the use of data more broadly. This has led directly to the emergence of personal data privacy legislation (discussed in Section 5.2 below)

Connected car data has been collected for many years. However, connected car data remains generally opaque to consumers, who have limited understanding of the rationale for its collection, the purposes for which it is used, and little or no perception of the scale, complexity or significance of the data market. In many respects the low level of public consciousness is comparable to that of the personal data market 4-5 years ago.

> *"I've been working for more than 10 years in the automotive data space - where OEMs have been collecting the data and dealerships have been intermediating the customer relationship. There's been an ongoing demand from customers to see the benefits from the data they KNOW are being collected."*
>
> Jessika Lora, CEO & Founder, CarForce.io

Many participants in this research consider it inevitable that the connected car data market, and the importance of PII within it, will soon become significantly more prominent. The risk is that it does so for negative reasons - like the wider personal data market before it. This could seriously compromise consumer trust, increase demand for privacy-related legislation targeted on the automotive sector – and lead to greater consumer 'opt out'.

1.1.1. Consumer trust risks issues

Risks to individuals stem from combining connected car data with some form of identifier so that it becomes PII. While this may enable more value to be created e.g. more personalised services – it also creates possible threat, which has the potential to undermine consumer trust.

Security risk

Failings in the collection, transmission or handling of connected car data could result in a data breach with information falling into the hands of bad actors. More seriously, malicious hacking of vehicle control systems could result in serious injury or worse.

Privacy risk

Connected car data enables driving behaviour, geolocation, etc. to be tracked, meaning detailed surveillance is possible – with all the 'big brother' implications and concerns that this brings. Connected car data could be merged with other datasets to enable re-identification of individuals.

Discrimination risk

Personalisation of offers or services could lead to discrimination against certain groups or behaviours. Where PII is used to target offers and services to individuals then the risks may be exacerbated.

The use of connected car data in automated decision making about the individual brings in the risk of algorithmic bias. This can lead to exclusion from a service or price discrimination.

Misidentification risk

If a system or process malfunction or erroneous data integration leads to inaccurate data being generated, there is a risk of harm to the individual due to flawed decisions being made. This risk is heightened by automated decision-making.

Inequity risk

The risk of connected car data being used to further the interests of businesses and their commercial partners rather than the interests of the driver. For example, if a driver asks the in-car assistant for directions to a gas station and they are given directions to the station of a provider who has used 'paid search' to gain favourable promotion, the customer may not receive the best price possible and will incur additional cost as a result.

"We know we deal with privacy across the board in multiple settings that are not necessarily about connected vehicles… but the risks are the same risks. A lot of the data that cars are collecting, and will increasingly collect, are very sensitive - precise geolocation or biometric data for instance… when you overlay that with a very complex ecosystem - it takes a lot of parties to create this environment - it becomes clear that you have serious privacy issues."

Omer Tene, Chief Knowledge Officer, IAPP

1.2. Implications of Data Protection Legislation and Regulation

Legislation is being designed and enacted to protect customers from risks associated with the inappropriate or unapproved collection of data and the misuse, mishandling or unintended exposure of that data.

Some of this legislation has been developed over an extended period, such as the General Data Protection Regulation in the European Union. Other legislation has been advanced in the wake of major data breaches and personal data usage crises in recent years.

Even where legislation has been in place for several years its practical effects on markets are still emerging. And where legislation is hastily constructed there is an increased risk of unintended consequences for data markets.

Data protection legislation to date has been developed to address the broad market of personal data collection, storage and usage. Unsurprisingly the legislation is influenced heavily by screen-based / internet / data platform models.

There is a risk that this could create challenges for other types of data markets, such as the data from connected cars - constraining innovation in this emerging market.

"The threat to connected vehicles is that these laws are being drafted principally with the data platforms [Facebook et al] in mind and with safeguards in place for that context [where] people can more easily understand what's happening in terms of what data they are surrendering and how they can keep control over that data once it's been collected. This creates significant problems in the automobile context - automobiles are not smartphones on wheels."

Harry Lightsey, Hawksbill Advisors

Connected car data may contain PII but it's fundamentally different from phone and browser data which monitors preferences, purchases, browsing history, etc so the legislation may not adequately reflect those differences. Also, the orientation of legislation around current dominant digital platform

models could also create an unintended advantage in the emerging connected car data market for the major data platform providers. This could lead to benefits not being shared proportionately among stakeholders, further stimulating data monopolies.

> *"The key question is 'What is PII'? Is it PII if it is used primarily for internal operations and optimization of vehicle performance? And should the CCPA be used as a model? The challenge for policymakers is finding the balance between providing consumers appropriate protections without creating unintended consequences for businesses that rely on certain types of data to enhance safety, security and quality of products consumers depend on. This nuance is challenged by certain legislative approaches but it remains a key concern for a number of stakeholders."*
>
> Charles Haake, Vice President and General Counsel, Global Automakers

The ways in which the user interacts with data and how it is presented to the user is very different in an automotive environment than it is using a smartphone. This creates significant challenges in implementing rights and obligations in a connected car setting. A major issue being the gaining of consent.

1.2.1. Consent

An effective and transparent consent model will be key in acquiring and maintaining consumer trust in this market. In the absence of such trust, the risk is that consumers will increasingly opt out of (or not opt in to) the collection and use of their data – limiting the development of the market.

Complications of consent and consent management, and emerging best practice

Consent and consent management needs to be clear and efficient. A poor user experience risks consumers becoming apathetic toward active consent management - negating the rationale for its existence. Consent must be granular to be specific, e.g. addressing consent to data collection, to data sharing or data sale, to the specific use cases for the data (as known now, and as can be anticipated in future)

Meeting these requirements presents challenges to the motor industry and the in-vehicle context, as the traditional approach of establishing an agreement with the customer at the point of sale of the vehicle does not address consent needs for data-enabled services. Within the vehicle, there are user interface and user experience challenges to providing sufficient information, obtaining the necessary affirmative action or dealing with timely and dynamic consent.

> *"It's likely you have to collect permissions up front in a CC data context as 'just in time' may not be appropriate e.g. due to the nature of in-car interfaces and safety concerns. But will this satisfy legal requirements – what happens if you change your mind or new services are layered in?"*
>
> David Le Duc, VP Public Policy, Network Advertising Initiative

Other key consent issues in the automotive context include:

- The user varies: the driver may not be the owner what are the rights of another driver / passengers?
- The user context varies: private vehicle / taxi / fleet operators vs fleet drivers etc.
- How to deal with new services being added?
- Multiple consents, possibly from different providers may be needed to permission a service or action
- How does revocation work?
- What happens when the vehicle is sold on (especially privately)?
- What happens when an intermediary or service provider, with whom the data is shared, establishes a new use for the data?

Emerging Industry Solutions for Managing Consent – BMW CarData and Connected.Drive

Approaches are beginning to emerge in the automotive industry which begin to address these consent challenges. One such example is BMW CarData.

BMW CarData allows drivers to manage and control connected car data collected from their BMW and Mini vehicles, and approve the sharing of this data with third-party service providers who use it to innovate new services for BMW and Mini drivers (see Section 7.3).

This approach to consent addresses many of the challenges outlined above. As part of this service, BMW and Mini drivers use their BMW Connected.Drive smartphone app to manage their consents with BMW and Mini on collection of data, and with the providers who use the data in delivery of their services.

A broader data marketplace provider such as wejo could take this approach further - enabling a similar service facilitating all necessary consent operation across a much wider range of OEMs, service providers and consumers.

1.2.2. Business Implications and Risks

All businesses that handle data in the connected car evolving ecosystem face potential regulatory and commercial risk relating to the collecting, storing and processing of data as part of their business operations. The growing use of PII has the potential to increase these risks by orders of magnitude.

The costs of maintaining the necessary data security, process and governance will escalate. Failure in this risks material reputational damage, with impact on customer trust, brand and market profile and business performance. Punitive fines for non-compliance with data legislation will also apply. e.g. the maximum fine under the GDPR in Europe is up to 4% of annual global turnover.

> *"In terms of when there is a data breach - and I say when because unless you've taken very strong privacy protective measures, you're going to have a data breach - then the damage to your brand and to your reputation is enormous, staggering."*
>
> Ann Cavoukian, Global Privacy & Security by Design Centre

> *"We have seen privacy become a central concern for businesses… so OEMs and more remote parties like car rental firms need to work out how to do data. If they don't, they are inevitably undermining and risking their business strategy and growth and it will be a detriment to them when the story comes out on the front page of The Wall Street Journal… telling how they are creating some awful privacy risks, or a cyber security issue. Those cyber security risks are very present and ominous"*
>
> Omer Tene, Chief Knowledge Officer, IAPP

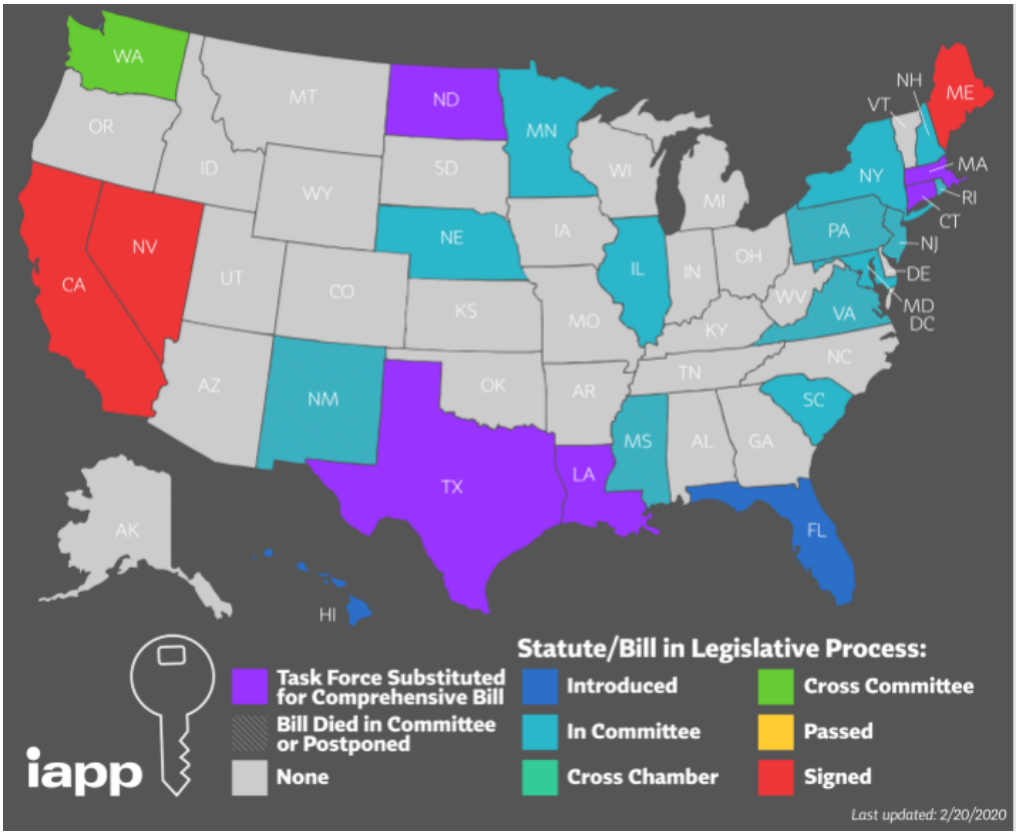
1.3. US Legislation and Regulation Related to Personal Data

The US legislative and regulatory landscape for the protection of PII has historically been fragmented. The US has generally regulated privacy primarily by industry, on a sector-by-sector basis. There has, however, been a shift toward more broad-based action on consumer privacy, in the wake of major data breaches and high-profile personal data market scandals.

States have taken the lead in implementing new legislation and this situation is expected to continue in the short to medium term as no Federal legislation is likely to be implemented before the Presidential and Congressional elections in 2020.

1.3.1. State-Led Activity

Current legislation and regulation activity at State level can be illustrated as follows:



The scope of the legislation enacted or being considered varies significantly in terms of the breadth of consumer rights enabled and business obligations imposed:

- Broad Scope: California, Hawaii, Maryland, Massachusetts, New York, Pennsylvania, Rhode Island, Texas and Washington
- Narrow Scope: Maine, Nevada, Illinois, Louisiana and New Jersey

California CCPA

California has been the prime mover in State-led legislation. The California Consumer Privacy Act (CCPA), inspired in part by the GDPR, has a broad definition of PII and what constitutes the sale of data. CCPA comes into effect in January 2020 and enforcement will start in July 2020.

Approach in other States active on data legislation

According to IAPP, the most commonly occurring consumer rights being enabled in other States are the right to opt out of data collection, the right to access data and the right to delete data.

Commonly recurring business obligations centre on the need to be transparent about data collection, and prohibition from discriminating against those who opt out.

There is a risk that state-by-state legislation, and potential variances between states, will add to complexity, and the compliance challenge to businesses that operate across a broad geography. However, this could be mitigated by a 'domino effect' with States replicating similar models to the CCPA - reducing inconsistencies across states.

1.3.2. Federal Activity

Whilst Federal legislation is unlikely in the near term, multiple comprehensive privacy bills have been introduced at the Federal level in the US Congress.

Whilst data privacy does not appear to be a partisan issue, the timing and potentially the nature (robustness) of Federal legislation will have a dependency on the outcome of the 2020 governmental elections.

There is the on-going potential for action by the Federal Trade Commission. The FTC Act allows the FTC to impose remedies for unfair and deceptive practices. It can issue fines when a firm has failed to adhere to a violation of an earlier consent decree imposed by the FTC. The recent fine imposed by the FTC on Facebook was high profile. It is notable that the settlement required Facebook to take a number of significant actions which could be seen as a good practice that other organisations will be encouraged to emulate.

If Federal data privacy legislation is passed and provides a level playing field – or minimum set of standards then this could help address the 'patchwork quilt' issues likely to arise from State-led legislation. Done effectively, this could provide the stimulus for interoperability, innovation and growth in the market.

1.3.3. Industry Self-Regulation

In 2014, the Alliance of Automobile Manufacturers and the Association of Global Automakers collaborated with industry to develop a set of Consumer Privacy Protection Principles which have become widely adopted in the automotive sector. The principles are set out in Appendix B.

While these principles are voluntary, by virtue of automakers' public commitments, they are enforceable under the FTC's consumer protection laws

This initiative demonstrates how consensus-oriented dialogue with industry, federal and state governments, and other stakeholders to address shared objectives, domestically and internationally can bring to bear practical, pragmatic and effective governance solutions.

1.4. Opportunities for Action on Trust and Legislation

The potential implications of consumer trust and data protection legislation and regulation for the US connected car data market suggest a number of inter-related areas where action could have meaningful impact on the development of the market.

1.4.1. Differentiation and leadership through Trust

There is an opportunity, to take the 'high ground' in this emerging marketplace and establish significant brand differentiation through trust – and putting the consumer at the centre. This could include:

- Demonstrably leading the market in the way that personal data is collected, stored and used with fair distribution of benefits to all stakeholders
- Living and breathing 'transparency', informed and practical consent, choice and education - including providing open access to tools that allow interested and expert parties to test security and privacy
- Working with recognised experts or organisations in the data privacy space to establish their advocacy - possibly including gaining specific 'accreditation' for particular products, services, processes and policies.

1.4.2. Actively promoting the benefits of the connected car data market

The opportunity to stimulate consumer and regulator confidence by raising proactively the positive profile of the connected car data market, and the benefits it conveys.

Recognising that consumers, generally have limited understanding of the rationale for data collection, and the purposes for which it is used, promoting the positive benefits of connected car data enabled services. In this way, contributing to building trust with consumers, on whose data the services depend.

Action in this area can help mitigate the risk and impact of the car data market becoming prominent for negative reasons that could seriously compromise consumer trust.

1.4.3. Working towards appropriate legislation

In addition to understanding and developing compliance strategies with legislation as it is enacted, there is the opportunity to positively influence developing legislation to support the beneficial use of connected car data for all stakeholders.

Potential focus areas include:

- Engage with state legislators to ensure that the unique characteristics of vehicle data and the beneficial use cases it facilitates are appreciated and reflected in new legislation.
- Work at Federal level to raise the profile of vehicle data and engage on a bipartisan basis to raise awareness and understanding of the sector.

1.4.4. Self-Regulation and Codes of Conduct

As vehicles are increasingly connected there is an opportunity for OEMs and other market participants to build both consumer and regulatory trust through reviewing and expanding their self-regulatory approach. This offers the potential to lead and influence collective thinking on the operation and regulation of the market through, the development of codes of conduct. Possible areas for exploration include:

- Potential refresh or further development of the auto industry Consumer Privacy Protection Principles to cover wider use cases of combined data types
- Extension of self-regulation to other industry players – building communities of interest

Conclusion

Connected car data offers significant benefits to customers as well as businesses, but it is essential that those customers know their personal data is safe. Attitudes about data collection have changed over recent years, and customers are now more aware of the potential risks. Emerging legislation has been designed to protect customers from inappropriate data collection and associated misuse and mishandling, and it is essential that providers are not only seen to follow that legislation, but also take an active role in its development.

Everyone in the connected car data market must work together to put the rights of the consumer at the forefront of all data collection, always securing consent and being transparent. By raising the positive profile of the connected car data market and the benefits it presents to consumers, providers can use this as an opportunity to build trust and foster better relationships with customers and regulators.

There are other challenges for the connected car data market, which will be explored in the next report.