Expert Insights

–

Securing privacy for the future of connected cars

IBM **Institute for Business Value**

Experts on this topic

György Halmos

György Halmos
EU Privacy Consultant
IBM Security
linkedin.com/in/gy%C3%B6rgy-halmos-dr-b73057145
Gyoergy.Halmos@ibm.com

György Halmos is a managing consultant for global privacy and EU GDPR matters on the EU privacy team at IBM Security. Mr. Halmos specializes in the privacy aspect of IoT, intelligent, and connected environments with special attention to connected and autonomous vehicles in the automotive industry.

Jayne Golding

Executive Consultant
European Privacy Lead
IBM Security
linkedin.com/in/jayne-golding-4300665
JGoldin1@uk.ibm.com

Jayne Golding is an executive consultant and the IBM European Data Privacy Consulting Practice leader, providing pragmatic privacy and data protection consulting services to Fortune 500 clients. Within the automotive industry, Jayne has significant experience in managing privacy and data protection within connected vehicle initiatives, including in-vehicle telematics services, infotainment services, insurance-based services, Smart Grid programs, and similar initiatives facilitated by IoT technologies.

> “Privacy by design is a holistic concept applied to operations across an organization or ecosystem, including its IT, business practices, processes, physical design and networked infrastructure”[1]

–

Talking points

Consumers demand privacy
Manufacturers should design privacy into cars that collect data. Sixty-two percent of surveyed consumers said they would consider one brand over another if it had better security and privacy.

No organization can single-handedly guarantee complete consumer privacy
Connected cars comprise components and systems from part makers, software developers, and integrators. They all can collect car data. Privacy takes an ecosystem.

Privacy can be a key differentiator
Don’t simply provide privacy. Promote privacy leadership while selling, on social media, even within the company.

Privacy in the connected car market

“If I had asked people what they wanted, they would have said faster horses.” This quotation, sometimes attributed to American car innovator Henry Ford, makes the point that customers don’t always foresee what they want. Or what might become technically possible. However, when it comes to privacy, users know that they want it, even if in the case of connected cars, they don’t know or care how it’s achieved.

The connected car market (see sidebar: What are “connected cars?”) was estimated to be USD 52.62 billion in 2016. By 2025, it’s projected to increase four times to USD 219.21 billion.[2]

According to a recent automotive study by the IBM Institute for Business Value (IBV), 56 percent of executives say security and privacy will indeed be key differentiators in vehicle purchasing decisions.[3] And in another recent IBV consumer study, 62 percent of consumers said they would consider one brand over another if it had better security and privacy.[4]

And, a third survey, this one of automobile and technology executives, mirrored the consumer findings. When asked to name the biggest obstacles to marketplace growth of connected cars, cybersecurity and privacy concerns came out number one, named by 31 percent – 50 percent higher than the next most-selected alternative.[5] And automakers are responding by investing in privacy. But a key question remains: are they investing in privacy wisely?

Recent global developments in the privacy regulatory landscape heavily affect the personal data processing activities related to connected cars. Among these, the European Union’s General Data Protection Regulation (GDPR) is perhaps the most stringent. It’s time for stakeholders of the entire connected car ecosystem, including manufacturers and their suppliers, insurers, retailers, and application providers to forego a piecemeal approach and undertake privacy comprehensively—an approach we call the principle of “privacy by design and default.”

Connectivity

What are “connected cars?”

A connected car is a vehicle containing devices that connect and exchange car data with networks and services inside and outside the vehicle, including those found in roads, homes, offices, businesses, other cars, and even with pedestrians and public authorities.

Connected cars are behemoths of data processing. They process up to 25 gigabytes of data per hour. Car software may include more than 100 million lines of code, far more than 6.5 million lines of code it takes to operate the avionics and support systems in a Boeing 787.[6]

What is the “connected environment?”

The connected car can communicate with five primary connection domains in the connected environment:

- **V2V** Vehicle to vehicle
- **V2N** Vehicle to network
- **V2I** Vehicle to infrastructure
- **V2P** Vehicle to pedestrian
- **V2E** Vehicle to everything

What data can be collected from a connected car?

Connected cars enable the collection of data about the vehicle—whether it’s technical, diagnostic or performance-based. These cars may also enable the collection of data about the driver and their use of: the car, any apps within the vehicle, and services, including traffic and navigation services.

It’s important to highlight that the collection of any of the data can sometimes directly or indirectly identify people, including drivers, owners, lessees or even passengers; therefore, the data isn’t only considered technical, performance, service, or usage data, but as personally identifiable information (PII). PII is owned by the user, so manufacturers and others—as processors—are required to comply with the relevant privacy regulations alongside customer expectations.

Privacy by design and default

Everyone in the connected car ecosystem needs to consider privacy a key element of connected cars, from designers and suppliers of subsystems, sensory environment, and applications; to manufacturers who integrate these components.

While some manufacturers and suppliers anticipate the demand for privacy, all too often, their actions are reactive. To address privacy challenges and evolving regulatory requirements, a paradigm shift has now become essential. The automotive ecosystem can’t wait to react. Instead, it needs to proactively plan and design for privacy, an approach that is embodied in the privacy by design and default principle.

Designing for privacy requires the participation of all entities that process connected car data and takes into account key consumer privacy considerations before vehicles are delivered.

> “Privacy by design is a holistic concept applied to operations across an organization or ecosystem, including its IT, business practices, processes, physical design and networked infrastructure.”

> “Privacy by default requires privacy embedded as a foundational setting so that even when customers do nothing, their privacy remains intact.”

> “Privacy by default requires privacy embedded as a foundational setting so that even when customers do nothing, their privacy remains intact.”[7]

Business aspects of privacy by design and default

Successful application of the privacy by design principle is becoming an important brand attribute of connected cars. Designing for privacy is a customer-centric approach that is becoming a powerful differentiator in purchase decisions and may help drive sales. In the connected era, privacy shouldn’t be treated as a secondary consideration (see Figure 1).

—

Figure 1

If data is gold, protecting data is diamond

1. Make privacy a brand of the intelligent car system (Develop your own vehicle privacy brand)
2. Advertise, promote, market, reference your privacy brand and achievements
3. Monetize your privacy brand and achievements and expertise

Applying privacy by design and default

Privacy by design and default requires the following fundamental management activities:

- Creating and coordinating mixed design teams of privacy experts, engineers, application designers, and legal experts
- Developing a design strategy
- Establishing and applying a proven privacy design and project management methodology
- Applying privacy enhancing techniques and technologies

A comprehensive approach to privacy by design and default

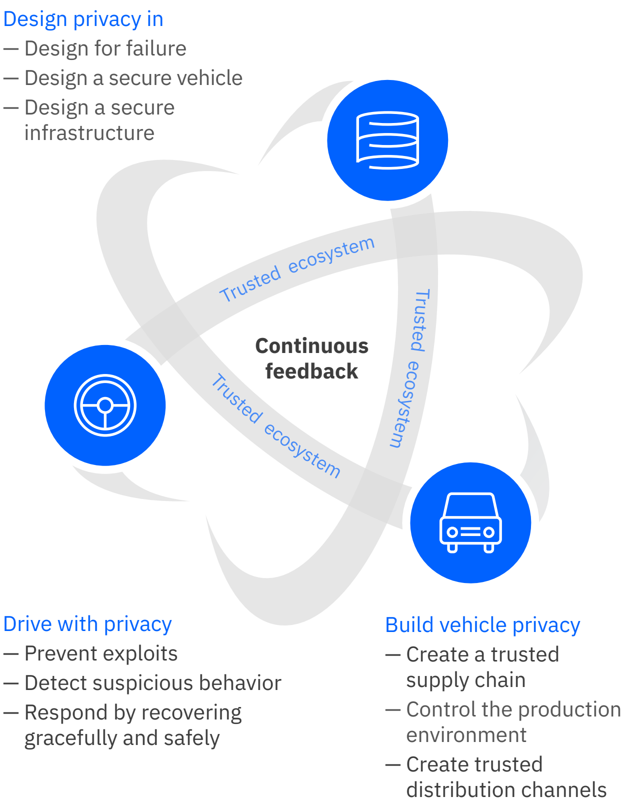
Enabling overall privacy in the connected car environment is a complex issue and undertaking. Privacy is best integrated through the three major phases of the vehicle lifecycle (see Figure 2):[8]

- Designing in privacy
- Building in privacy
- Driving with privacy

—

Figure 2

A comprehensive approach to privacy


Design privacy in
— Design for failure
— Design a secure vehicle
— Design a secure infrastructure
Trusted ecosystem
Trusted ecosystem
Trusted ecosystem
Continuous feedback
Drive with privacy
— Prevent exploits
— Detect suspicious behavior
— Respond by recovering gracefully and safely
Build vehicle privacy
— Create a trusted supply chain
— Control the production environment
— Create trusted distribution channels

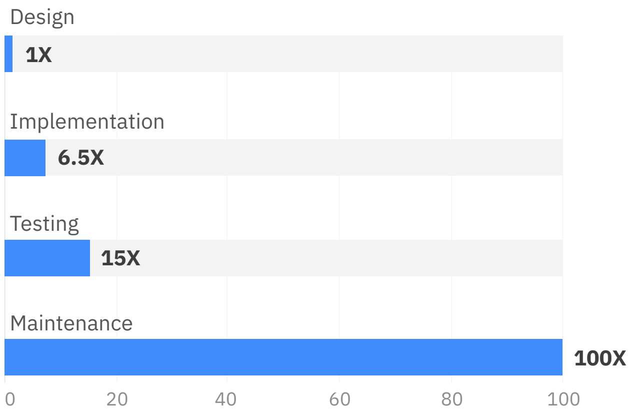
Designing privacy

A study showed that finding a software error in the design phase costs less than a sixth of the cost of finding it in the implementation phase, 15 times less than during the testing phase and 1/100th of the cost as in product maintenance (see Figure 3).[9] Realizing this underscores the importance of addressing security requirements as early as possible.

All too often, privacy is designed separately from the rest of the automobile. Or it's eschewed during design and left as an integration task during manufacturing. While manufacturing for privacy is a vital task, omitting privacy from design becomes a problem when suppliers change. New processes create integration problems, which can drive up costs. When privacy is a design point, many issues are weeded out at the earliest stage, at a lower cost, bearing in mind the interest of the user (data subject) and brand reputation.

Figure 3

Relative cost of fixing defects



Building privacy

Even when privacy is a design point, it remains a key part of the manufacturing process. The good news is that most of the OEMs are transforming their businesses to support privacy. But they sometimes lack a holistic, overarching approach to embedding privacy within the entire car lifecycle. For now, that responsibility lies with the manufacturer.

Building privacy starts with a trusted manufacturing environment for the automaker and its supply chain. Preventing and finding threats that might lead to privacy breaches in manufacturing are much less costly in dollars and reputation than finding them as the result of a customer complaint or in maintenance.

Driving privacy

Most of the "heavy lifting" to incorporate privacy features should be completed in design and build, before the driver gets behind the wheel, or the passenger enters the ride share. But the moment of truth occurs when these phases encounter customer expectations and experiences. Privacy should be the default without customers taking any action. Moreover, navigation, Bluetooth and onboard, interactive telematics shouldn't only enforce privacy, they should also promote it.

For many customers, the connected car is becoming an extension of their homes and offices. In many cases, they expect other devices they use while in a car to conform to the same privacy standards as the vehicle itself.

Build systems that can monitor events and perform analytics to detect failures and suspicious activity that may indicate a privacy threat.

Getting in gear to design—build—drive

Car manufacturers can take a few straightforward steps to integrate privacy:

- Create mixed design teams, choosing the appropriate privacy by design strategy, methodology, and technologies for cars' lifecycles. Doing these things can put you ahead of the changing landscape of regulation and requirements instead of constantly chasing it.
- Be diligent that you and your suppliers build systems that can monitor events and perform analytics to detect failures and suspicious activity that may indicate a privacy threat.
- Consider joining or creating a privacy ecosystem comprising suppliers, dealers, insurers, and key electronic device makers. Consider including after-market parts makers and even regulators. They all can be a part of privacy by design and default. Be a part of the standards-making process, not a victim of it.
- Remain customer-focused. Being a leader in the connected car market not only will keep your customers connected to their environments; it will help them remain connected to you as well.

Key questions to consider

» What steps are you taking to address the growing requirements for privacy?

» How are you managing access, ownership, and protection of the data that is collected by connected cars?

» In what ways is your organization working across the ecosystem to design privacy, and doing it as early as possible in the product lifecycle?

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Notes and sources

1 Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles." Privacy by Design. Jan 2011. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

2 "Connected Car Market by Service (Connected Services, Safety & Security, and Autonomous Driving), Form (Embedded, Tethered, and Integrated), Network (DSRC, and Cellular), End Market, Transponder, Hardware, and Region - Global Forecast to 2025." MarketsandMarkets. 2017. https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html

3 Stanley, Ben and Kal Gyimesi. "Automotive 2025 - Industry without borders." IBM Institute for Business Value. January 2015. https://www.ibm.com/thought-leadership/institute-business-value/report/auto2025

4 Unpublished data from IBV survey on: "A new relationship—people and cars."

5 "2017 Connected Cars & Autonomous Vehicles Survey." Foley and Lardner, LLP. 2017. https://www.foley.com/files/uploads/2017-Connected-Cars-Survey-Report.pdf

6 Charette, Robert N. "This Car Runs on Code." IEEE Spectrum. February 1, 2009. https://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0

7 Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles."Privacy by Design. January 2011. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

8 Poulin, Christopher, Giuseppe Serio, Ben Stanley. "Accelerating security: Winning the race to vehicle integrity and data privacy." IBM Institute for Business Value. January 2017. https://www.ibm.com/thought-leadership/institute-business-value/report/acceleratesecurity

9 Dawson, Maurice, Darrell Norman Burrell, Emad Rahim, Stephen Brewster. "Integrating Software Assurance into the Software Development Life Cycle (SDLC)." Journal of Information Systems Technology and Planning. January 2010. https://www.researchgate.net/publication/255965523_Integrating_Software_Assurance_into_the_Software_Development_Life_Cycle_SDLC

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
April 2019

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an "as is" basis and IBM makes no representations or warranties, express or implied.