The New State of Data Privacy:
Q&A With Jake Ward of Data Protocol

As part of our ongoing series about data privacy, we wished to better understand the "new state of data privacy" and specifically the roles, responsibilities, and investments of private companies ("privacy as a product") and developers ("privacy by design") in the consumer privacy space. Here, we interview Jake Ward, Co-Founder and CEO at Data Protocol. You can follow him on Twitter at @jacobmward.

How do you think the landscape of the "new state of data privacy" currently looks with regard to the roles, responsibilities, and investments of private companies and developers in the consumer privacy space?

Up until this point, the privacy consumer space has invested in prevention – fifteen billion dollars was spent on privacy tech startups in 2021 alone. But this "gold rush" drives an assembly line of off-the-shelf automated privacy point solutions rooted in way-too-late forensic reviews. This is a mistake. In prioritizing detection over prevention, privacy tech attempts to mirror security solutions, treating privacy as a bug as opposed to a feature. Privacy violations and data misuse are the result of human decisions; a technology solution cannot be applied to a behavioral problem. Instead, developers must be empowered with the knowledge to partake in the compliance discussion long before issues arise. By giving developers the tools and information to drive prevention, it can become foundational.

This is a growing - and meaningful trend. Look at what Google is doing with Checks. This is an internal effort to leverage AI technology to identify possible privacy and compliance issues within apps. But foregrounding prevention requires a common set of skills and language among legal, product, and engineering that we're just not seeing, yet. Before we launched Data Protocol, I conducted workshops with developers who build consumer facing products that rely on data from platforms and partners. In each of these workshops, across countries and experience levels, I learned that most data misuse doesn't happen because of malfeasance. It is caused by ignorance or desperation. The absence of knowledge and options is what causes mistakes. The solution is a higher standard of training and more resources readily available.

What is "privacy as a product" in your opinion? For developers and other technical professionals, how does "privacy by design" (or "privacy engineering") play a role in building "privacy as a product"?

As I see it, privacy isn't a product - it is a feature of every product. And it should be reflected in three dimensions. Firstly, it activates the right mindset, meaning that if we train developers and require companies to treat privacy as a core feature, then it will get prioritized. Secondly, it meets consumer expectations. A recent study from Cisco showed that 86% of consumers care about data privacy and want more control and 79% of consumers are willing to invest more time and money to better protect their privacy. And finally, privacy as a feature drives competition. The U.S automotive industry was completely resistant to incorporating safety features until the Motor Vehicle Safety Act was passed in 1966. Now the industry competes vigorously around safety features. Privacy is the new safety feature of the digital age, and the time has come to provide the safest products.

Privacy by design was created to serve as a broad set of principles that guide policy conversations. But it falls short in providing developers a practical path to building products responsibly. Privacy engineering aims to fill this gap by making privacy by design an actionable practice. As a field, privacy engineering encompasses the technical architecture, methodologies, and systems in managing data that achieves privacy protection. That is what led us to launch the publicly available privacy engineering certification program with goals of training and certifying every developer in the world. Every developer should be a privacy engineer.

To what degree do developers currently practice or prioritize data privacy in the product development process? How do you think this will evolve over time?

It's a common misconception that developers don't care about data privacy. They do. Of course they do. They are proud of their work: they are parents, and consumers themselves. They care about privacy as much, if not more, than anyone. Last year we conducted a study over over 1,000 North American developers and uncovered a critical paradox: 70% of developers think protecting consumer data is important. But 73% feel pressured to make coding decisions that compromise data privacy. This is even more common (80%) with developers at startups. So it's not that developers don't care, it's that they haven't been empowered with the knowledge they need to prioritize data privacy. We need to make data management and privacy skills easier to learn than they are to ignore.

Developers with an understanding of how to protect their products and users are the best line of defense against misuse, misteaks, and malfeasance. And they do want that line of defense. The problem is, most data management and privacy education programs for developers are terrible. They offer linear, slide-based learning experiences built on the legacy learning management systems used to teach sexual harrasment training. We can do better. Data Protocol supports, teaches, and trains developers the way they want to learn - in an propulsive live terminal environment. This is too important not to do well.

This is the second Q&A in a series that DCI is publishing on the topic of Privacy Tech to better inform and engage policy and business stakeholders who are both influencing and influenced by these new dynamics in the privacy landscape.