Vita Zwaan is a senior associate at the law firm bureau Brandeis, leading their Privacy Team. She is specialized in compliance issues with regard to privacy and data protection, telecommunications, e-commerce, the liability of internet service providers, free speech, and intellectual property. Vita also stood at the forefront of changes made to the so-called Cookie Law to make it more flexible, and argued some of the most groundbreaking cases regarding the liability of internet service providers.

Internet of Things regulations are complex and challenging.

We asked Vita Zwaan, a senior associate at the law firm bureau Brandeis, the key questions which organizations face when they go to market with IoT solutions.

Who are your customers and how do you help them?

A lot of my work is related to new media and technologies. I assist companies, offering technology and services to end users, to deal, among others, with compliance issues. Think, for example, about video, retail, or telecommunication services. Several parties are involved, working with technologies which have an influence on the privacy of citizens and the end users. I assist those parties in the compliance field. I make sure that what they design and put in place stays in line with the regulations. It is better to think about those aspects upfront instead of first developing products and afterwards finding out that there are issues.

I work with in-house company lawyers, but also with other departments, such as communications or research and development. The way the product or service is presented to the end user is critical and involves those different disciplines.

What is the biggest risk for your customers?

One of the biggest risks for the companies I assist is that they might fully comply with regulations from a legal point of view, but could still fail with their product if they fail in their communication to the end user. Let me explain this in more detail. Connected objects and services are gathering data from their users. Companies usually ask consumers for their consent to access and store such data, which is needed to operate the service. From a legal

point of view, you can say that this company is acting within the law. But it is also critical to communicate and explain to your customers what you intend to do with this data. If you do not, consumers and media might jump on it and it could get out of hand for the company involved. Remember the bad press around the smart meter or GPS services monitoring your location? The consumer perception of those innovative data-based services is critical. Companies providing those solutions could even be at risk of going out of business if the end user somehow feels manipulated.

Are there specific Internet of Things (IoT) laws or regulations? Are such regulations taking place at European or national level?

There are currently no specific IoT laws or regulations, but there are guidelines and opinions from advisory authorities in Europe, as well as the U.S. Such guidelines are issued by different regulators. For example, privacy and telecommunications authorities. There are no guidelines including all possible regulations yet, but they might come in the future.

An example of such an advisory authority, in the field of privacy, is the Working Party 29 (WP29), made up of representatives of all EU member states. WP29 provided an opinion on how it thinks businesses in Europe should comply with privacy regulations.

Privacy laws in Europe are embedded in an EU directive which was drafted in 1995. At that time, it did not take into account the latest technology developments, not even the internet. We are still applying European laws that were written when people were working with paper-based databases. Europe has just released a new regulation which will be applicable as of May 2018. We will then have a completely new privacy framework in the EU, which will not need to be implemented as part of national laws, but will be applicable to all EU citizens or, for example, large US companies operating in the EU.

Until this new directive in the field of privacy has been enforced, advisory authorities are able to tell us how to interpret the 1995 law in today’s world and can help to work towards new legislation.

Which domains are relevant and should be considered as part of an IoT regulations quick scan?

Privacy, which we just mentioned, is a very important aspect. I would also name telecommunications laws and intellectual property laws.

Security is also important to consider and falls partly under privacy laws and partly under telecommunications laws. This aspect is not handled in a separate law. Those are the main ones. Topics such as personal data ownership or retention fall under the privacy laws, basic civil law or most likely under intellectually property laws in regard to copyrights, patents, or trademarks. Another aspect might be liability. If you offer a data platform or technology, on top of which your customer is building an end-to-end application, it is important to define who is responsible if it goes wrong.

Lastly, but not to be forgotten, is criminal law. All data collected by an end-to-end IoT application might be requested by law enforcement. The police might not only request you to provide data on when an end user called someone else and what they discussed, but also, for example, where they were, where they drove, when they were using electricity at home, or even whether they were healthy. Such information is now available with IoT sensors.

A law proposal in The Netherlands will allow the police to hack end user equipment to check what they are doing. This is, of course, something that citizens are concerned about and it is important to keep in mind that there should be limits to what is collected and how long this data could be stored.

A last example is a Dutch law which makes it mandatory for companies to notify the regulator if they have been hacked or had their data breached. This obligation is important to know as a company.

How should I get started on regulations as a company? Keep in mind that some of those companies are small and have no telecom, IT, or data experts.

As a company, it is important to understand whether your plan, product, or service stays in line with regulations.

The first step I usually take with my clients is to understand their project or plans. For example, I use questionnaires or presentations, and I try to involve not only the technical or business departments but also others like communication. As a regulations expert, I need to

understand in which legal framework and categories the application falls into, while my customers need to understand what they have to do. After those interviews, I provide a short-list of possible implications and how to deal with them. Awareness is also important, so I sometimes give presentations to the whole company. I usually stay involved for a longer period of time to help this company make decisions along their IoT journey.

An important good practice is privacy by design. While developing your IoT application, keep the end user in mind and the fact that he/she should always be able to take decisions in regards to privacy. Your IoT solution should support those choices. It is easier to define and implement those at the beginning of a project rather than running behind once the project is too far. Take those options from scratch in your requirements, in your technical solution, and in your process definition. Consider the following example: a company is informing their customers that they can request to have their user data deleted if they stop using the service. This sounds like privacy-friendly good practice. It is also very easy to implement as long as no customer requests it. But it also means that this company should be able to remove this specific customer data if the customer does request it. In practice, it might not be as easy to realize considering the fact that such IoT services are using lots of different partners and databases. So make sure you take this requirement with you even before starting to design and to select partners.

What if your company is not going to design the IoT service itself but make use of partners and third-parties? Does it need to worry about regulations?

In this case, your company has to worry about the agreement that it can put in place with other parties involved. Your company will be the party that will be addressed if a problem arises with an end user. Therefore, your company should select their partners wisely so that it complies with consumer laws while servicing its customers. It needs to have the liabilities in place where they should be. Even though they do not design anything themselves, they still need to be able to ask their potential partners the right questions and put the liabilities on paper in their contracts. Your company should be aware of these aspects.

The Internet of Things can be categorized in different application types, also called "verticals" – for example: automotive (cars, transportation), mobile health, factories, and energy (smart grid, smart meter). Do specific regulations apply for

each vertical?

Yes, different regulations apply depending on the use case. Take, for example, a mobile health application collecting data from a consumer. This IoT solution, from a privacy law perspective, is considered very sensitive for two reasons. Firstly, because the product involves an end consumer and secondly, because it is related to health. Therefore, a whole set of strict regulations apply. A second example is automotive; safety aspects are probably involved and therefore, regulations protecting the end customer's physical integrity.

The key to each vertical is to assess the application from a consumer point of view. How could such an IoT application impact the consumer and which regulations should apply? The more a consumer could be impacted, the stricter the rules.

If you had to give one piece of advice to a company decision maker in the field of regulations, what would it be?

My advice would be this: Empower the end user! Make sure that your customer or end user is fully informed about your product and its implications. Empower this user, allow him/her to make real choices. In particular, privacy by design and by default should be in place on day one of your IoT journey. If not, you are running the risk that your product or solution might be labeled as unsafe or un-free by consumers or the media, and bring your whole plan and ambitions to a stop!