How to Make GDPR a Threat Again

Nikolai Horn in Conversation with Dagmar Hoffmann and David Waldecker

Abstract *Dr. Nikolai Horn is an expert for data protection. He has worked for the Foundation for Data Protection (established by the German government). Currently, he is a political advisor for iRights.Lab, a German think tank which deals with the legal and policy aspects of the digital sphere. The interview is a follow-up conversation after Nikolai participated in a round table on smart speakers and data protection at University of Siegen. It covers legal and political aspects of data protection regulation with regards to voice recordings.*

Dagmar Hoffmann (DH): What are the main problems with data protection with regards to voice interfaces?

Nikolai Horn (NH): First, we have to look at what personal data is relevant in this case and if there is a legal frame for dealing with the type of data and its use cases. That is, are we talking about recorded speech? And we need to consider if this recording can be considered personal data. And yes, we can consider it to be personal data because it can be used to identify the individual speaking. However, we also need to see if it is sensitive data. Article 9 of the European General Data Protection Regulation (GDPR) lists "special categories of personal data" (GDPR Art. 9), such as the sexual or political orientation of an individual, or its health-related data. Here, data processing is tightly regulated. I would suggest that recorded speech can be considered sensitive personal data in the sense of art. 9 for two reasons. Reason one is that recorded speech can be considered biometric data as it allows to identify an individual in the same way that fingerprints do. Second, recorded speech can be analyzed for health aspects of

the speaker. Thus, it is personal and sensitive data. It requires explicit consent to be processed and the GDPR restricts certain forms of analysis of said data.

Also, the goals of the data processing and its context have to be considered. Again, certain use cases of recorded speech can be relevant for data protection. Recorded speech could be used for profiling; it could also be used to analyze speech patterns in order to create a personalized artificial intelligence (AI) model of an individual speaker. This would allow for another dimension of abuse. That is, with a growing risk of misuse of data, there has to be a higher level of protection, especially when it comes to recorded speech.

DH: We also have to consider how error-prone this speech recognition still is nowadays. When somebody calls me, it is hard for them to tell me and my daughter apart, but AI is able to do so?

NH: By now, AI is able to do so. This is obvious with regards to today's programs generating pictures and videos – and video is a lot more complex than audio to generate. For a good simulation of a speaker, current software needs to analyze maybe five minutes of recorded speech. The more audio available, the better the simulation is. A potential use cases is radio broadcasting: It has been suggested to replace newscasters and anchor persons on radio stations with AI after having analyzed recordings of their spoken words. Concerning your example: the better the algorithm has been trained, the better it can distinguish between you and your daughter based on really short samples of speech.

Right now, the EU is debating how to regulate AI. In order to tell artificial and human speakers apart, some suggest to create a watermark that highlights the artificiality of computer-generated speech. Also, one could think of an AI-based algorithm which can tell human and simulated speakers apart.

David Waldecker (DW): In our view, it is this potential of AI-based speech recognition and processing which is often not known to users of smart speakers and voice assistants. There is a lot of public debate on issues of data protection. Research done by others and ourselves has indicated that users are aware of this debate, and in our interviews (cf. Waldecker/Martin/Hoffmann, this volume), they often asked us if we planned on talking about this aspect of smart speaker use. However, concrete knowledge about the potential use cases of recorded speech and its economic potential seems to be lacking. Users we interviewed suspected that data from smart speaker use might be analyzed for the personalization of advertisement on other platforms. Smart speakers,

at least until now, do not play ads, but the more popular models are part of platform companies like Amazon and Google which might actually use this data in the way suggested. We wonder, if there are other use cases which are economically viable and how these are problematic from a data-protection standpoint.

NH: If we look at use cases of natural language processing (NLP) – the AI method used to generate, understand and analyze human speech and writing – a number of points are worth mentioning. As the broadcasting example shows, it can be lucrative to automate speech. Also, it is relevant for data protection because somebody's personal data has been used here. However, it is also interesting to ask from a philosophical point of view: Who does somebody's voice belong to? That aside, speech analysis is also an interesting aspect because there are several potentials for application. Next to the ad placement you mentioned based on speech analysis, we can also think of the analysis not only of the content, but the speech itself, i.e. the analysis of feelings and the psychological state a person is in. This is technically possible and it could be used, e.g., for political advertisement. It could also be used in job interviews in order to automatically analyze the manner of an applicant. There is one real-life example of the Bundesamt für Migration und Flüchtlinge (BAMF), the German federal agency responsible for asylum claims and related matters. In an experiment, this agency had applied an AI speech analysis to discover if an applicant's dialect, in, say, Arabic, matches the country or region that the applicant claims to have come from originally. Here, we see the problem of this application. Critics were concerned with the use case itself and the methods applied; also, the system turned out to produce a lot of errors. These mistakes, if undetected, would have had serious consequences for the applicants.

Also, this AI audio technology could be used for surveillance purposes. For example, it could be used to find out who was present at a meeting of a group of people. There are innumerable scenarios for application. However, there are also potential benefits in the early detection of diseases and disabilities which are present in speech but usually go unnoticed. These forms of detection should conform to data-protection regulation, but maybe one day our cell phones could analyze our conversations on the phone and suggest visiting a doctor at some point. This sounds horrible to some, but it could be created in a non-threatening manner. So, advertisement really is not the most spectacular application I could think of.

DW: In passing, you mentioned the question of who one's voice belongs to. How would you answer this question?

NH: This is an interesting topic. To a certain extent, companies nowadays treat personal data and an individual's voice as a person's property which she can transfer to others. However, I find this economic perspective and the idea that spoken words are property misleading because it suggests that one can sell this data or information in some way. When we consider speech as a biometric marker, i.e. my individual way of speaking, my personal grain of the voice, so to speak – then we do not consider the economic aspects of property, but the legal aspects of ownership and control over something. Here, constitutional law and the fundamental rights of a person become relevant. These rights are not for sale. Thus, I cannot sell my fingerprint, or my voice, for that matter.

DW: Well, you highlighted a number of ways of analyzing speech as data. For us, the interesting thing is that – with all the potential inherent in speech analysis – the actual commands issued in our interviews to voice assistants were often quite trivial. Users often use their smart speakers to turn music or the light on or off, or they ask about the time or the weather. So, some users we interviewed suggested that their use is harmless from a data-protection standpoint, because their commands do not convey any personal or sensitive data. Also, they suggested that the data is analyzed by companies like Amazon or Apple who know about their habits anyway, by analyzing their shopping and online query behavior. In this sense, we were wondering if this public discourse on the surveillance of speech and the domestic sphere relates to an actual danger or to an much more benign phenomenon?

NH: I think this debate is not over. One phrase that comes to mind is "rational apathy." This term suggests that users are looking mostly for short-term benefits, like a more comfortable remote control for the living room lights, while not thinking about the long-term consequences. Of course, it is hard to anticipate the ways data about the lighting in private homes can be used; but even in this case, pattern recognition could be used to the detriment of the user – without them even knowing about it. Another example would be the simulation of individual speakers: You only need a couple of minutes of somebody speaking for a good simulation; this technology has been used in impersonation by criminals. However, it would be too much to ask for the average user to know about and to think through all these technological consequences.

As you mentioned, it is true that companies like Apple, Google and other platforms already collect a lot of data anyway. We do not know what these companies use the data for, and we do not know if they follow data-protection guidelines. Thus, it is doubtful if regulation for data protection is being taken seriously. And because users are unable to control the flow of data, it is questionable if "informed consent" is a correct descriptor of the actual situation when digital services are used.

I have been working in this field of data protection for a while now. In everyday life, I cannot think of many cases where I do know and understand how the data is being processed that is being collected. With certain companies, users can take for granted that their data is being kept in a closed system with high levels of security. With other companies, users and citizens cannot be so sure what happens to their data, for example with certain smartphone companies or with an app by a non-European company. It is unrealistic to assume that everything is processed according to the GDPR. It should, because users in Germany reside in the European Union, but certain companies and providers are based in authoritarian states where this legislation is hard to enforce. And so, before wasting too much time on this issue, users simply take it as a given – asking themselves "Why should something happen to me?"

DW: You mentioned a number of negative consequences. When we asked users about the potential problems of using a smart speaker, they were aware of some of these problems and stated that they would not mention banking account numbers and passwords in front of the device. So, there is this attitude of nonchalance you mentioned, and there also is this feeling that the device is harmless and has not caused any greater problems. From this point of view, one particular user suggested that anyone who is concerned about the data processing behind smart speakers and voice assistants has fallen for conspiracy theories in the vein of believing that vaccines actually inject nano robots into people's bodies. That is, this problematization that we are discussing here is very distant to certain users. On the other hand, all these problematic data practices you mentioned – how much do they really affect people in any way they can directly experience? And even if they do, how problematic are they for these users? It seems that the legal perspective is too removed from everyday life to matter. To a certain extent, the legal aspects you have mentioned are somewhat fictitious. In order to create the possibility for informed consent, every user of a smart speaker or even an activated voice assistant on a smart phone would have to inform every visitor or everybody in the vicinity about an active device

and the consequences of data processing. Empirically, this is not the case. So, already in the everyday use of the device, legal obligations are not kept up with, neither by users nor the manufacturers.

NH: Well, this is one of the main problems. NGOs and other actors have tried to make data protection a popular issue, to get people concerned about it. De facto, these debates are only something for experts. Experts know about the potential problems and actual cases where things went wrong – for example in a case of a children's toy which recorded interactions with it. And before the activities of Cambridge Analytica became public, their application of Facebook's potential was somewhat the matter of fiction, too. Now, this is reality we have to deal with. We just have to ask ourselves, if we want to wait for another scandal of if we want state agencies to create certain boundaries and norms proactively.

I do not want users to be forced to think about data protection, instead I want users to be able to trust experts and agencies to take care of potential pitfalls in digital data processing. This kind of oversight should work like it does with cars: As a driver, I do not need to know how a combustion engine works, but I need to be able to trust the agencies that inspect and certify cars for their safety. Thus, I do not need to know if and how the breaks or a valve could malfunction as long as experts and governing bodies take care of these risks by countering them by prescribing high standards for quality and safety. I think that we need the same procedures for voice-related technologies, before they can get easily exploited by criminals.

Getting to this legislation and regulation will not be easy because it is hard to anticipate every scenario where users could be at risk. This is obvious with the EU AI Act where certain areas, such as human resources, are considered high risk, but it is complicated to imagine risks in all potential and future areas of application. This borders on technology assessment procedures where you asses concrete technological products. It is hard to exactly determine the risk connected to a particular piece of technology, especially with this type of technology and its wide field of application.

DH: While it might be hard to assess these current technological trends, Amazon and Google products nowadays enable users to listen to the recorded interactions, i.e., to view their technical interpretation and the answer or results. It is also possible to comment upon or even delete this data. Most of those interviewed did not even know about the possibility, neither to assess the recorded

data, nor to delete it. We wonder if this is some kind of pseudo-transparency and ask ourselves, like some of our interview participants, if it is worthwhile to delete these recordings?

NH: This feature in certain smart speakers relates to the discussion concerning article 20 of the GDPR and the "right to data portability". Here, the GDPR stipulates that the "data subject" should be able to receive a copy of all the personal data saved about the subject by some organization and that the subject should be able to transfer this data to another entity. While this was hailed by some as a means of consumer sovereignty, it turned out to be a somewhat toothless piece of regulation. Google had implemented this possibility before the GDPR took effect, because it does not cost much to implement and because it is pretty useless for the individual user. Google has done what it was asked to do, so I do not blame Google. Instead, I wonder why data protection agencies thought this kind of regulation would be useful. Why do we need things like Privacy Information Management Systems (PIMS) or privacy enhancing technologies which focus on the individual user? I would suggest that we need to enable organizations, such as consumer protection agencies or NGOs like AlgorithmWatch, to analyze this data and to press for charges in a class-action lawsuit. I think that it is much more productive to look for ways to enable users to realize their rights on a collective basis than to provide them with technical tools that are only interesting for the individual experts, if at all. So, we have to look at the legislative aspects but also at the implementation of the regulation itself. We do have enough regulation in the abstract, calling for privacy by design or privacy by default, but we are lacking best-practice examples. And while it makes sense to be skeptical of Google and other companies in the field, we might even develop tools together with those companies which allow for a greater and more meaningful control of personal data.

DW: This is interesting as users currently often are left with the choice to accept the vague and obscure data policies of a digital service or to not accept them – which means the inability to use the service. It is this dyadic relationship between platform and user that leaves the user solely with a choice to "take it or leave it." You mentioned NGOs as trust-enhancing organizations. What do you think of institutionalizing data management in a triadic fashion?

NH: I dealt with questions like these in 2017 as a member of the "Stiftung Datenschutz" [Foundation for Data Protection]. In a research paper (Stiftung

Datenschutz 2017) on new directions in consent in data protection, we examined PIMS and their connections to digital ecosystems. So, I am not up to date on the state of the art concerning tools which, for example, manage the consent forms for users on different platforms. I also wonder if these tools that are offered are in use in any meaningful sense – just because you provide a handy software conforming to the GDPR, it does not mean that users integrate it into their everyday activities. So, we need to find out how to deploy and use these tools to have a lasting impact. That is, we need more research, in line with behavioral economics, but also in a more interdisciplinary setting. In addition, what we need is effective and powerful agencies able to enforce legislation and regulation concerning data protection. As public offices in this field are notoriously understaffed, we might need to resort to class-action lawsuits or a more coordinated effort with consumer protection bureaus. Essentially, we need to find ways to combine the legal possibilities inherent in this legislation and we need to foster new and powerful forms of regulatory oversight.

DH: Earlier in this interview, you suggested that users should be relieved from thinking about data protection at every turn. What can we ask users to do then, concerning voice assistants and data protection?

NH: While information and education are important, I am a wary to turn towards schools to educate our future citizens on these matters. This will help to a certain extent but will not get the job done. I think that we have to make digital products which adhere to privacy standards more appealing. This will allow for a better position on the market. Apple, for example, has been advertising its products as more secure and protective of personal data. This leads to greater trust in the brand as well. In the end, data protection should become one of the main reasons to use or shun a product. Data protection must not be viewed as an annoying hindrance, but as a protection of fundamental rights. Those digital products that protect (digital) fundamental rights and enable the exercise of these fundamental rights most effectively deserve respect and must be recognized as such. Maybe, with the advent of AI and the current debates in the dangers inherent in its ubiquitous application – maybe this will lead to a greater sensibility and a demand for products which are more attuned to data protection.

Translated by David Waldecker

References

Stiftung Datenschutz. 2017. "New ways of providing consent in data protection – technical, legal and economic challenges. Leipzig." Policy Paper. Available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/Video/Fremdveranstaltungen/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_PolicyPaper_New_ways_of_providing_consent_in_data_protection_EN_final.pdf