Journal of Law and Health

Volume 35 | Issue 3 Article

10-15-2022

Transcript: Presentation on Individual Autonomy in AI Healthcare

Charlotte Tschider
Loyola University Chicago School of Law

TRANSCRIPT: PRESENTATION ON EXPLOITATION AND INDIVIDUAL AUTONOMY IN AI HEALTHCARE

Presented By: Charlotte Tschider[1]

The Journal of Law and Health's
Digital Health & Technology Symposium

CLEVELAND-MARSHALL COLLEGE OF LAW
FRIDAY, APRIL 8, 2022

[1] Professor at Loyola University Chicago School of Law

The following is a transcription from The Digital Health and Technology Symposium presented at Cleveland-Marshall College of Law by The Journal of Law & Health on Friday, April 8, 2022. This transcript has been lightly edited for clarity.

Charlotte A. Tschider:

First of all, it's wonderful to be amongst such fantastic scholars. I am so thankful to the students and the organizers of this publication. It is a great privilege to be able to discuss these topics with folks who are deep in figuring out what the right solutions might be.

I wanted to share a little bit of background about how I have gone down this path before I jump into the details. Dr. Krista Kennedy, of Syracuse University, and myself have worked extensively on analyzing the relationships between individuals and devices, especially pervasively attached devices like hearing aids.

As part of that research, we combed through blog posts, communications between data scientists and others in organizations. As we did this, we realized the concept of "datafication," which is the digital rendering of a person as representative of data. For example, if you have a person's data, that independent data might be treated differently than if a human being is sitting in front of you. We saw the concept of datafication in blog entries, where data scientists attempted to use as much data as possible or create devices to collect as much environmental data or as much behavioral data as possible.[2]

Something did not sit quite right about this practice in the context of medical devices. Many individuals are dependent on medical devices. This begs the question – will the medical device offer better treatment or a better diagnosis than we might have otherwise achieved without that same amount of data? Should we have to have a corresponding negative impact to the individuals who use these devices, even though the patient or their insurance have already paid for it?

These considerations brought me to question: what does exploitation look like in this space? And is it possible to connect the concepts of data loss and excessive data use to this concept of patient exploitation?

To address these issues, I like to start with the technology. It is always super exciting to discuss the underlying technology. We have smart hearing aids and insulin pumps. There are a lot of diagnostic efforts around the imaging space. There are also many surgical robots; some that are more complex and some that are more specific for a particular purpose. Artificial intelligence is not something far

[2] For more information on "datafication" *see e.g.* Margarita Shilova, *The Concept of Datafication; Defination & Examples*, DATA SCIENCE CENTRAL, (June 2, 2018, 1:30 p.m.) https://www.datasciencecentral.com/the-concept-of-datafication-definition-amp-examples/.

off in the future, it is something we're using today. So, the issues associated with it are things that we really need to prioritize and think about from a legal perspective now. One of the biggest problems is that data is essential for the creation and function of these devices.

In some cases, there may not be representative data which may lead to a disproportionate impact on certain populations, including safety issues that affect certain populations more than others. The idea is that data is essential to safety, and for useful development of artificial intelligence, that data must be identifiable. We often need this type of data over a long period of time, not just at a point in time. As you can imagine, when you have a device that somebody wears for a long period of time, seeing how effectively that device functions (for example how accurately it predicts insulin dosages) over a period of time would be more valuable to future product development than how it behaves and makes decisions at a specific point in time.

So, we know that we need data. We know that we need representative data over a long period of time. How do we achieve that while guarding against data overuse that could trigger potential privacy risks? It is helpful to understand the size and expansion of these big data set implementations that we are talking about and what data could be most useful in these spaces.

The first type of data, of course, is medical data. This includes information about individuals' past medical procedures and different diagnoses, and this data is very useful. Additionally, behavioral data about patients – what they eat every day, who they interact with, how social they are, how active they are – can be tremendously useful for something like insulin delivery. Kinetic data, like where they are going and what situations they find themselves in, is particularly useful for devices like hearing aids because we want hearing aids to easily adapt to a person's environment. So, being able to sense and then actually analyze the data to automatically adjust is an important part of how we design those devices.

Another big area of expansion is secondary use – how can we use data to create new devices, how can we use data for other purposes. Pre-pandemic, I visited a company in Finland that was looking to use data for multiple purposes. They had collected data for a particular type of glaucoma test, but they thought they could use it to predict Alzheimer's Disease. However, they were not able to use the data for those secondary purposes because they didn't have consent from the individuals, which seems right to us. But there might be situations where a data reuse is actually in the best interest of individuals. So how do we manage all these pieces?

Let's start with the problems.

The first problem is the idea that we do not exactly have a traditional fiduciary role with relation to A.I. technology. This can give you a sensation of a

false trust. What I mean by this is: suppose you have a manufacturer creating an A.I. technology, an individual who is using the A.I. technology, and a doctor in the middle. Now, if the doctor doesn't really understand how the technology works, then presenting potential privacy risks to that individual is going to be very difficult. But because a doctor is prescribing the device, there is a sense of trust that comes with that, and unfortunately, manufacturers benefit from that trust.

We also have the issue of sensitive data collection. Certainly, the types of data we collect through many of these devices are not publicly available. We are talking about very sensitive information. For devices that are always on like hearing aids, you might be collecting information about the individuals a person associates with. You might be collecting intimate details. There is a lot of information that can be collected from a hearing aid that is not collected through traditional medical records today.

Another problem is exigent health events and a lack of analog alternatives. When a person is seeking use of an A.I. medical device, whether it's for a diagnostic purpose, a treatment purpose, or it's a device that a person pervasively wears, they're doing it often because it's the best option or because they must. This is not a situation where we have discretionary choices – where somebody can simply choose a different coffee maker. Unfortunately, when someone must choose between their health and their privacy, they are usually going to choose health.

Even if we provide patients with all the information, the health choice is almost always going to rank a little bit higher. Couple that with this idea that data is so useful and so necessary that there is an incentive to collect more, we ultimately have a lot of issues for the individual. The individual is sort of "riding in the backseat," and the technology is really riding up front. This means is that we have a risk of exploitation – we are taking something from an individual and not really compensating them for it.

Now, I do not necessarily believe that market solutions are the best way to manage privacy. I think there are a lot of dangers in that. But basically, the idea is that the act of taking someone's data, of replicating their data, and then sharing their data with third parties, when the individual is not aware of it or does not have meaningful choice, can in and of itself be called a deontological risk, even if their data is not misused on the back end and even if their data does not lead to some significant cyber event, like identity theft.

And so, I think if we reframe this as an autonomy problem, we can potentially get some solutions that are better than simply plugging in consent and saying we're good with that. Consent really can't cure these issues because of all the things that I have just talked about. Simply providing information is probably not going to be accurate or informative enough to really motivate individual choice. As I have written about in the past, we have major issues with consent anyway, in

part because individuals are faced with so many privacy notices in their lives that it is very difficult to comb through all of them and really understand the salience of the potential privacy risks associated. When a collection and variety of different behaviors exceed what we would consider our normatively accepted values for a community, exploitation can result, and when there is exploitation, we should be requiring organizations to do more to overcome that risk to individuals.

Let me describe an example of what data sharing can look like in an average health care system. It all starts with device data, even if we're talking about something simple like insulin pump function. That data goes between a variety of organizations, from a clinical hospital, to the manufacturer, to the doctor, to A.I. startups providing the A.I., which is also actually used by the manufacturer. A lot of this data, eventually, will make its way to insurers or to joint ventures between clinics, hospitals, and other third parties. In the center of it all, of course, you have this doctor and patient. A lot of patients really don't understand the inner workings of these details behind the scenes and how their data might be duplicated or used.

So really, the bottom line is that the potential risks in data sharing are really difficult to communicate. And when we have complex A.I. systems, like unsupervised deep learning systems or anything similar, unfortunately, those risks are especially hidden in the data. There is an inherent opacity, and you have a change in those algorithms developing over time, so even an explanation that could help us in one moment will probably be different in the next moment as that A.I. continues to change. How could we manage the situation in a way that is based on information? A privacy notice for information that an individual must take into account when they are presumably in a health situation where they're trying to make a decision in the best interest of their health it is just not really a great fit.

One of the movements in privacy law recently, more generally than just health, is the idea of an information fiduciary.[3] The way this idea has been framed is that individuals or organizations who receive personal information should act in the best interest and in loyalty to that individual.[4] And while I am a little bit skeptical of how this could apply across the board for any consumer related transactions, I do think that healthcare could benefit from an expanded conception of the fiduciary role. It doesn't necessarily have to operate like existing fiduciaries.

However, one of the things that we must take into account is the idea that there should be some type of relational duty. Because we might have a doctor in the middle, but the doctor is not really somebody who can explain potential risks in a way that is very salient. Or, they also are not really in a position to change the

[3] For more information on "information fiduciaries" *see e.g.* Adam Schwartz & Cindy Cohn, *"information Fiduciaries Must Protect Your Data Privacy*, ELECTRONIC FRONTIER FOUNDATION, (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy.

[4] *Id.*

nature of the technology or the nature of the data sharing that's occurring. So, developing a relational duty between the manufacturer and the individual is really important here.

One of the ways that we can think about doing this is by establishing the role statutorily, under a health privacy statute. We have a variety of different state laws that focus on healthcare privacy that extend HIPAA in some important ways. We also have a variety of different technologies that do not actually fall under HIPAA. Consumer healthcare devices, in particular, could be subject to health privacy statutes, even where they wouldn't be subject to HIPAA requirements.

We could also consider ways to bolster risk assessment requirements. Under HIPAA, for example, we do have a requirement to conduct risk assessments from a privacy and security perspective.[5] It would not be that difficult to add in an additional risk assessment related to the potential for exploitation of downstream patients. One of the things that I have talked about previously in my writing on other projects is the idea of legitimate interest analysis.[6] One of the ways we might be able to overcome these limitations in consent is to focus on the legitimate interest of the particular individual, a community of individuals, or potentially within the public interest as a way of demonstrating that additional collection or data sharing is going to be in the best interest of the individual.

Now, the most important part here is that you would have to publish this somewhere, so that it can be inspected, whether that be by a separate regulatory body or the general public. I think it is really important that if we are doing this kind of analysis, it is published somewhere. There are many ways we can evaluate legitimate interest here. We could think about resource availability. We could think about representational data that could overcome potential discrimination issues. There could be efficacy or safety concerns, but we want the potential legitimate interest to outweigh the commercial interests of the organization. There are also different methodologies that have been shared in the EU and other places that can help us do this in a systematic risk assessment-oriented way.

The core question here is: is the data used primarily for the individual or is it for the business? What should organizations do if they cannot demonstrate legitimate interest? Well, we have some options and I think the best option is to use de-identified data. Currently, I think a higher standard is needed than what HHS

---

[5] Nat'l Coordinator for Health Info. Tech., *Security Risk Assessment Tool*, HEALTHIT.GOV, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool#:~:text=A%20risk%20assessment%20helps%20your,PHI)%20could%20be%20at%20risk. (June 3, 2022).

[6] Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model*, 21 HOUS. J. HEALTH L. & POL'Y 125 (2021).

requires under the identification safe harbor.[7] They certainly could use anonymized data or synthetically-created data. You could purchase publicly available data sets that are not protected health information. You could create research data sets yourself and invest in that. You can rely on data donation or philanthropy of individuals donating their information. And, finally, though maybe not the best option, you could purchase data in these situations. There are plenty of ways we can get around relying completely on individuals and poor tactics to swindle data away from patients when patients really are dependent on good care and quality health results.

[7] For more information on "HHS Kickbak Rules" *see e.g.* Harold B. Hilborn, *HHS Issues Revisions to Safe Hornbors Under Anti0-Kickback Statute*, THE NAT'L L. REV., (Mar. 5, 2021), https://www.natlawreview.com/article/hhs-issues-revisions-to-safe-harbors-under-anti-kickback-statute.