1. Data Collection and Use SAMPLE REPORT

Our model uses data collected from previous customers, which they agreed to provide for what we described as "research and product development" purposes. The data contains information about identity (age, gender, marital status, education, occupation), family information (number of driving children, children at home), SES (income, home value, neighborhood), behavioral history (claim frequency, car use, revoked license), and vehicle information (car type, car value, car age).

Ethical Challenge

Any time that companies make use of data from human subjects, they must ensure that this data is collected and used in a respectful way. A rights-based approach will advocate explicit consent from data generators,[i] but this is rarely done in practice. Instead, companies more often rely on some form of blanket consent (e.g., "I give permission to use my data for purposes chosen by the company") or implied consent (e.g., "by using the platform or posting information in public view, the data generator consents to its collection and use"). Some positive-rights approaches will also care about whether the data generator would have hypothetically consented to the particular use of data.[ii] For example, in the Cambridge Analytica scandal, the company may have used data for political marketing to which the data generators would not have originally agreed.

Importantly, all of this assumes that the data subject has and maintains rights over their data, as a form of either property[iii] or identity,[iv] as described in the GDPR.[v] Yet it may be the case that data generators do not have rights over data at all, or they may transfer these rights to the company permanently.

In a consequence-based approach, data is not viewed as a right but rather as sensitive information, and consent is less important than impacts. As such, some data may be so sensitive or harmful that it would be wrong to use it even with consent (e.g., health information). Additionally, some purposes may be so important (e.g., national security or public health emergency purposes) that it overrides refusal from the data generators.

A new challenge posed by AI systems is that the use of data to train a model may not explicitly appear in the output of that model.[vi] Instead, the model will "learn from" the training data, and it's not obvious whether this requires consent in the same way as traditional data collection and use. For example, companies like Google and OpenAI argue that they are able to use the work that artists post on their website for promotional purposes as training data, even when that material is protected by copyright laws.[vii]

Standard

There are several standards that companies could adopt in our case, which range from requiring explicit consent from each previous customer for the use of their data in this particular AI model, to not requiring any consent because this data is only used to train models or because it was

previously transferred to the company and is now our property to make use of in any way we choose. The standard that our company is using to design this AI model is:

> *We will attempt to contact each data generator to notify them that their data is being used for training an AI system to make recommendations to customers and agents about pricing for new customers. We will offer data generators the choice to opt-out of this usage within a reasonable window of time, after which it will not be possible to remove their data's impact on the model.*

This standard represents a moderate view on the spectrum of possible positions described above. We expect that most data generators will not object to their use of data in the training set, and this will have little or no impact on the performance of the model. In addition, we expect that customers will appreciate having control over their data, even when used for training models.

Arguments and Objections

We believe that the training data is not the property of data generators, and that they do not have full ownership and control over it. Thus, as opposed to the GDPR's "right to erasure," we do not think that data generators have the right to demand removing the impact of their data on a model after the training phase (indeed, this would be practically difficult or impossible). However, we do believe that the training dataset contains important information about the identity of the data generators, and we therefore have an obligation to respect the dignity of the data generators by making a due care effort to ensure that this use does not violate their values. We hypothetically assume as a default that any reasonable person would not object to the use of their data for this purpose. If we don't hear from data generators after sending notice, we can assume that they would have agreed if asked directly. However, we include the opt-out feature as a sign of respect for the fact that the dataset contains information about their identity.

One might object to our standard by questioning how we could possibly know what data generators would hypothetically consent to, and why it is reasonable to assume that everyone would agree to this use. We respond by noting that this data was originally collected by an insurance company for "research and product development" purposes, which could be expected to include AI systems for pricing. The fact that data is used to train models now constitutes common knowledge. In addition, the purpose of building pricing models is not harmful to data generators or anyone else, and is indeed beneficial for customers and the company alike.

Another objection is that this opt-out approach places an undue burden on customers, who may not understand the nature of training data and the value that it creates for the company. This exploits the inertia and lack of attention or expertise on the part of data generators, and provides the illusion of consent. In response, we note that we are not requiring actual consent for training data, but only providing notice as a sign of respect for the identity of our customers and their role in the training data. We concede that this is a minimal gesture, but the use of data does not depend on agreement in this case.

[i] Brennan, J., Jaworski, P. (2015) "Markets Without Limits: Moral Virtues and Commercial Interests." New York: Routledge.

[ii] Nissenbaum, H. (2004). "Privacy as Contextual Integrity." Washington Law Review 79, no. 1: 119-158.

[iii] Merges, R. P. (2011) *Justifying Intellectual Property*. Cambridge, MA: Harvard University Press.

[iv] Radin, M. J. (1996). *Contested Commodities: The Trouble with Trade in Sex, Children, Body Parts, and Other Things*. Cambridge, MA: Harvard University Press.

[v] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[vi] Fazlioglu, M. (2023). "Training AI on Personal Data Scraped from the Web." International Association of Privacy Professionals (IAPP) Blog.

[vii] OpenAI Comment Letter (Oct. 30, 2023), https://www.regulations.gov/comment/COLC-2023-0006-8906; StabilityAI Comment Letter (Oct. 29, 2023), https://www.regulations.gov/comment/COLC-2023-0006-8664; Meta Comment Letter (Dec. 6, 2023), https://www.regulations.gov/comment/COLC-2023-0006-10332; Google Comment Letter (Oct. 30, 2023), https://www.regulations.gov/comment/COLC-2023-0006-9003.