



Voice Data Collection Must Be Transparent

Consumers need to know whether their data will be used, and for what purpose

Increasingly, data is being collected at a distance without the individual's awareness, raising a multitude of issues. Companies employ a "more, more, more" mentality, without regard to the consequences.

In 2015, cloud computing traffic was estimated at 106 exabytes per month in North America alone, and global Big Data revenue is expected to grow to nearly \$34 billion this year, according to Statista.

We can try to put the genie back in the bottle, in part by ensuring data collection is fair and protects the privacy of subjects. Because, remember, it's not just the user whose privacy is in jeopardy. If a doctor is dictating patient notes using cloud-based speech recognition, privacy concerns are implicated for him, the patient, the patient's family and friends who may be included in the notes, the referring physicians, other care providers, and the like.

A mathematician who has written algorithms for companies including AT&T and YouTube acknowledges that while companies may be overreaching—silently collecting exorbitant amounts of user data, including speech—he does not necessarily believe the companies have nefarious intent.

But nefarious intent is not the issue; fair data-collection practices are. And ensuring that requires a framework of new and existing laws.

The Federal Trade Commission (FTC) has the authority to enforce consumer protection laws, including unfair or deceptive acts or practices.

A practice is unfair if it is likely to cause substantial injury to consumers that consumers cannot reasonably avoid and that is not outweighed by benefits to consumers or competition. Thus, if data is sold to a purchaser that has bad intent or if a data breach harms the dictator or the party mentioned in her dictation, this could trigger the unfair practice prong.

If a company says "We give you a choice whether or not to give us your data; click here" but the company does not say "also click here," it's a deception issue.

Depending on how a company is collecting and using users' speech files, the practice(s) could be unfair and/or deceptive.

Earlier this year, Vizio entered into a \$2.2 million dollar settlement with the FTC for engaging in unfair and deceptive practices—tracking what people watched on TV without their consent, after providing only vague disclosure of what it was doing.

Collecting Big Data

Why would companies keep voice recordings of doctors talking about patients?

"It may be a way to get information regarding particular

consumers or to see trends," says FTC attorney Peder Magee. Companies could track occurrences of health conditions, types of medicines being prescribed, or which doctors are prescribing the meds.

The value of this information is astronomical. A 10 percent increase in data accessibility translates into an additional \$65.7 million in net income for a typical Fortune 1000 company, according to Baseline.

Imagine pharmaceutical companies accessing this information to target doctors who are prescribing competitors' medicines or to see who has gained weight since last year's physical, then sending coupons for weight-loss products.

It's already happening. Hospitals can now increase revenue by selling patient data to aggregators that process the data, creating a colossal database and leveraging the data for a monthly fee. This could generate millions

of dollars annually for a hospital.

A lawsuit against Charter Communications this year alleged that its products and services were not being offered for or provided at the total dollar rates advertised because Charter failed to disclose it would receive valuable consideration for selling subscribers' information.

Consent

With so much data being collected surreptitiously, how can consent even be possible? And what about companies such as Nuance that state they may use user data for any purpose, maintaining the data indefinitely?

"Data uses that are not transparent are secret uses of data," says Marty Abrams, executive director of the Information Accountability Foundation.

No privacy principles allow for secret uses of data if there are no established parameters for the individual to understand what the data is used for. "That's not using data in an ethical fashion," Abrams says. And almost all privacy principles say companies should not use data beyond its effective life. "Maintaining data forever is not a good answer."

Magee believes consumers should have meaningful choice whether or not to share their information. Notice should be given based on the consumer, the intended use of the data, and the type of information being collected. Consumers need to know how companies are going to use the data and if their information is going to be shared in a different industry or context. ☒

Nefarious intent is not the issue; fair data-collection practices are.

Robin Springer is an attorney and the president of Computer Talk, Inc. (www.comptalk.com), a consulting firm specializing in speech recognition and other hands-free technology services. She can be reached at (888) 999-9161 or contactus@comptalk.com.