Acoustic Data Ethics Principles

April 2021

acoustic

Marketing technology, reimagined.

acoustic.com

OUR DATA ETHICS MISSION

Ensure the integrity of our data practices and be a thought leader for our customers.

Purpose: *At its core, data ethics means ensuring the use of data is not just legal but also ethical and fair. It is a more expansive view of data privacy and protection—not just the privacy compliance and the technical infrastructure for data protection, but also the governance, the trends and ethical questions that evolve as technology and norms change and evolve. It means having an ethical data use framework throughout the data lifecycle phases, including how we collect, store, use, share and delete data, as well as the accuracy and quality of that data. The overarching principle is trust: we are entrusted with data and we need to treat the data in a way that continues to engender trust.*

What we believe:

- Trust is earned — from the public, customers, consumers, partners, regulators, and each of us within Acoustic.
- Data practices must be human-centered and in the service of people, not machine driven, and balance needs and preferences, not just algorithms and regulations.
- Consumers must be empowered—empowered to learn how information has been gathered, stored, and used and to obtain the information about them that is online.
- We must understand and strive to meet the expectations of data subjects — those people about whom we are gathering information. We aim to treat people's data the way THEY want it to be treated.
- The data supply chain should be transparent. At every step — collection, use, storage and destruction — and with every change of hands. The process through which we handle information should be clear and reviewable by anyone with a valid reason for seeing it.
- We can lead the way for our industry. We lead by being a company that fully lives up to its code of ethical behavior and also by helping our customers and the industry understand the importance of data ethics and how to incorporate these data ethics into a company's business processes.

How we act:

I. We protect the customer and consumer data that our customers have entrusted to us and our platform

As a marketing cloud provider, our customers entrust Acoustic with their own customer data, often consumer data. This starts with a privacy and data ethics-by-design approach, so our customers have the tools to meet their own customers' expectations. If the consumer's trust is violated, that potentially damages both Acoustic and our customer.

A. Earn and value public trust. This includes the trust of our customers, their consumers, our partners, our regulators, and each of us within Acoustic.

1. Do what we say. Acting inconsistent with what we have represented will break down trust.

2. Do what the consumer (aka "the data subject") expects. Satisfying expectations might even be more important than being perceived as law-abiding. If we continually disappoint, our customers can walk away.

B. Legal compliance is the minimum bar we must clear.

1. Laws usually follow the technology and public sentiment. Violations are not only a matter of legal repercussions, but also a matter of reputational integrity. As important as following the law is, we need to be ahead of it--our data ethics practices should anticipate where we and the market are going.

2. We follow the spirit, not just the letter, of the law.

C. Security, transparency, and enabling consumer control are our core priorities. We must incorporate best practices in data privacy and security to be in the best position to prevent a potential data breach. The consumer must be told clearly what information is being gathered, for what purpose, and have a straightforward way to correct any erroneous information.

D. Privacy of data.

1. All of the data that passes through our platform is confidential. Whether it's Personally identifiable information (PII) or buying habits, all is personal, sensitive, confidential information. PII is not just names and phone numbers but can also include, for example, health information, GPS location, or financial transactions. Even publicly available information, like what you might find in the phone book or on a company's website, can become sensitive when combined with other information, like the name of a healthcare provider or a financial institution.

2. A data breach would not only be a legal problem, but it could also put Acoustic at a competitive disadvantage by negatively impacting the Acoustic brand and reputation.

3. When we use data to derive trends and improve our products and services, we de-identify/aggregate/anonymize the data. De-identification/anonymization means removing specific information such that it no longer is capable of being associated with a particular individual or household.

E. Security of data.

1. Confidentiality and availability. There are valid third-party uses for confidential information, such as the sharing of financial information between partners or in consumer transactions, but this sharing is only to be done with all needed safeguards in place and with clear agreements. There must be correct handling of data throughout the data lifecycle at all stages of processing including availability and encryption, as appropriate. Confidential data is encrypted while traveling over public networks, and while at rest when stored. Confidential data is protected from the time it is collected and through its lifecycle within Acoustic products and systems.

2. Integrity. Data must be gathered and stored in a way that assures its accuracy, traceability and lineage (source) to provide transparency and auditability. This is not only a moral and legal imperative, but also a business one, since we should not be conducting business with faulty data.

F. Data ethics by design.

1. We build products and services with data ethics at their core, including privacy and security by design. We will align privacy and security measures and safeguards with the highest reasonable expectations, and we do this in part through our product design, where we will institutionalize the expectations into the product to support controls and safeguards.

2. Security and proper handling of data is not added on at the end of the product lifecycle: security and privacy requirements are built into all products, solutions, and processes from the start. For example, our data science and product management professionals meet with the Data Privacy Officer during the early planning stages any time a product change will potentially impact data practices.

3. Incorporate transparency. Knowing that partners, regulators, and consumers could have a need to know how data is gathered, handled, and stored, the ability to easily review all data processes should also be built in.

4. Configurability. Our aim is to build our solutions with security by default, so they can be straightforwardly configured, without options that could introduce security shortfalls.

5. Accountability. Our solutions are built so that it is clear what person, process or tool is responsible for each step in gathering, using, and storing data.

6. Auditability. Every product/solution we build must have a clear interface, capture data access logs and other audit information, and have tools that will make review of the data processes clear.

7. Clear disclosure of technologies. We provide our customers with the clearest explanations of the technologies employed by Acoustic, so that our customers can disclose these clearly and accurately within their policies, opt-ins and notifications.

II. We support our own customers by:

a. respecting and protecting the business and personnel data they provide and that we use to market and sell our products to them;

b. helping our marketing customers incorporate best practice principles when they use our platform

For our direct customers — the marketers who buy our solutions — we have a responsibility to carefully handle any data we collect from them and they entrust to us. In turn, when they become our customers, we give them the tools to meet these same responsibilities with their own customers. But more than that, we guide and assist customers, partners, and even regulators, to ensure that our solutions are used successfully and appropriately and also to provide thought leadership around use of data.

G. Human-centered design. To assist our customers, we emphasize human-centered data design and practices so that their data collection and use is responsible, both legally and ethically. People are at the center of what we do and all deserve fair and equitable treatment.

H. Control and consent

1. Data ownership by consumers. While we and our customers might be gathering consumer data, it is the consumer who owns her or his personal data. We hold the data in trust. We require consumer permission — "opting in" — to gather and use that data. As well, our DPO works with our product team to promptly respond to data subject "do not sell" and "right to be forgotten" requests.

2. Empowerment of customers and consumers. At any time, the consumer may request to learn how information has been gathered, stored, and used so that our customers can promptly respond to their consumers.

3. Responsiveness. The longer sensitive data is incorrect or inappropriately visible, the more of a frustration or danger it is to the person who owns that data — the consumer. Correction of misinformation must be completed as soon as possible.

I. Transparency

1. Algorithms and machine learning. Learn and be prepared to explain the workings of algorithms and machine learning — how the technology works.

2. Downstream uses. Consider and disclose downstream uses, such as what is done with the data sets, or re-purposing. Be mindful of "invisible" processing (where data is enriched and enhanced without the consumer's knowledge). Since we are responsible for how the data is handled, we remain responsible for any downstream use of the data. This has particular relevance with machine learning and AI processing where we aggregate, score or unify different data sets.

3. Sharing, selling and buying data. Be sure you know when it is permissible to share data-- with Acoustic sub-processors, sub-contractors, and data partners— or to sell data to or purchase data from third parties. For instance, is it permissible to use cookies or other third party tracking technology? These decisions should be made in collaboration with the Legal department and, where appropriate, the Chief Data Ethics Officer.

4. Audit trails. Capture and store the context of collection, consent, inter-company transfers, and the history of decision-making from raw data to processed data and data set.

5. Data supply chain visibility. Be prepared to explain how the data travels through the data supply chain, including data's lineage/provenance.

6. Data minimization. Data minimization and limitation are critical to mitigate the risks of unforeseeable downstream or future use of data. Gather only what is needed and appropriate and retain it only as long as necessary. This is a situation where less may be more: gathering more than is needed or reasonable could endanger individual privacy and lead to reputational and other issues.

J. Profiling / Data analytics

1. We will not interfere with human will — that is to say we will not make inferences that aren't there, and we won't use data science to create compulsion or addiction to use any product or service. We should be thoughtful and deliberate about which predictions and inferences should be allowed and which should not.

2. We are aware of the potential to manipulate data with algorithmic amplification and must incorporate checks on this potential. We are in the business of marketing, but we also have a social responsibility for how our tools are used.

K. Bias institutionalization (AI)

1. We're cognizant of vulnerable population impact. For example, data can be a tool of inclusion or exclusion. We help guide marketers to account for and correct bias.

2. We strive to mitigate any disparate impact of our products, if any, on vulnerable populations.

3. We respect the people behind the data, with extra care for the gathering, use, and storage of data.

4. We pledge to be thoughtful about the intent behind and impact of algorithms. Who is being excluded? Are the people included being pushed into an "echo chamber"?

5. We recognize power relationships-- whether that is the large corporation dealing with individuals, especially vulnerable populations, or dominant players in the industry setting a bar too low-- and will not permit any power dynamic to adversely impact our data ethics.

L. Set standards. We collaborate with our data science professionals to establish and enforce professional standards and accountability.

M. Organizational "anchoring"

1. We have established a data ethics office, led by our General Counsel & Chief Data Ethics officer and our Data Protection Officer.

2. We seek to train and empower customer-facing teams to speak confidently about Acoustic's data ethics. Our data ethics are in fact a brand differentiator. Our customers recognize the value of careful and ethical use of consumer data.

N. Data ethics governance and ethics review

1. Internal. The "first line of defense" should be peer reviews. If you have any questions, contact our General Counsel and Chief Data Ethics Officer, Sharon Zezima.

2. External. Stay abreast of new uses of data and the questions they might raise. Consider forming an advisory board of external data experts and thought leaders to ensure objectivity and access the trends and innovations in the area of data privacy, security and ethics.