Nobody Owns What Was Said

A constitution for memory

Version 1.0, November 2026. Published by Recordist, which makes an app that keeps a record of calls, and so has an interest in the argument that follows. Dedicated to the public domain under CC0. This document is not legal advice.

recordist.app/constitution

1. One sentence

A client on a video call tells her adviser that her marriage is ending, and that this is why the money has to move by Friday.

He asked at the start whether he could record, so that he could look at her instead of at a notepad, and she said of course. So the meeting service has her voice. A speech model turns it into text, and a language model boils the text down to a line that reads, Client divorcing, funds to move by Friday. A search index takes that in, so that anyone at the firm who types the word divorce will find her. Next month an agent reads it and drafts a follow-up. When he deletes the meeting, a backup keeps it. A lawsuit against the service, which has nothing to do with either of them, may require that it be preserved, and then the service is sold.

Everyone in that chain may have behaved perfectly well, and she knows about almost none of it. She thought she was talking to one person.

He may have a duty to write it down, and her husband's lawyer may one day ask for it, and neither fact makes it the company's. Some of this chain survives a move to software on his own machine, ours included.

Now ask who owns the sentence. The company's terms probably say that the customer owns its content, and then license it broadly. He pressed record, so he probably assumes it is his. She would not understand the question. For most of history a conversation ended when the people in it stopped talking, unless someone wrote it down in plain sight, and as far as she knows this one ended when she hung up.

2. What changed

Forgetting used to be the default, and remembering took effort and money [1]. Manners and law grew up around that fact.

Now it costs less to keep everything than to decide what to keep. Years from now someone can find her sentence in a second, with the morning she said it gone from around it. A system can work out from her words things she never said, and the reader most likely to open it next is software that can act on what it reads.

None of this means the best conversation leaves nothing behind. People are held to their word by what was kept. Someone who has died is still in a voicemail on an old phone in a drawer, and nobody who has one of those thinks of it as data.

By *memory* we mean any lasting trace of what passed between people that a machine made or holds. That covers a recording of voice or video, a message thread, a transcript, a summary, an embedding and a gesture caught by a camera, along with what is made from them, such as a score or a model. A set of trained weights is a memory from which no one can yet reliably remove a single person, and the US Federal Trade Commission has ordered a whole model destroyed instead [19]. What a person remembers or writes in their own words is different, because a person can be asked to account for it. Court records and journalism have older rules of their own.

3. The predicament

Custody. Whoever holds a memory can be subpoenaed, hacked, bought or shut down. Under the US third-party doctrine, information a person voluntarily hands to a business has long been treated as outside the protection of the Fourth Amendment. The Supreme Court refused to extend that rule to phone location records in *Carpenter* in 2018, and again in *Chatrie* in June 2026, where it compared location history to emails stored on a company's servers [3]. The rule has not been overturned, and a warrant or court order can still reach what a custodian holds. In May 2025 a US court ordered a major AI company to preserve conversation logs it would otherwise have deleted, including chats its users had asked it to delete, because of a copyright case those users had no part in [4]. The general order ended that September. Accounts tied to domains the plaintiffs had named went on being preserved, and the logs already set aside, apart from those from Europe, stayed set aside. Later that year the maker of a personal memory product was acquired, switched off capture in its older app, and withdrew from the European Union, the United Kingdom and five other countries, giving people there two weeks to download their information before their accounts were to be permanently deleted [5]. Custody can also count against privilege. In February 2026 a federal judge in New York held that a defendant's exchanges with a consumer AI service were not privileged. The service was no lawyer and no lawyer had asked him to use it, and the judge added that its privacy policy, which let it train on them and disclose them, left him no reasonable expectation of confidence [20]. A custodian's promise lasts as long as the custodian's circumstances.

The way out. A memory that cannot leave is a very good way to keep a customer, because the longer you stay the more of your own past you would have to abandon to go. Section 7 shows where our own export stands.

Absorption. Models can retain and reproduce pieces of their training text [6], and short of retraining from scratch, there is still no general way to remove one person's data from a trained model [7]. So training is an act of custody that deletion cannot reliably undo. What a model learns from one adviser's calls also changes what can be guessed about every client like her, and nobody on that call can agree to that for the others [22]. The staff of the US Federal Trade Commission have warned against quietly rewriting promises not to train on what customers give [23].

Inference. A system can claim to read mood from a voice and attention from a face, although the EU's own lawmakers record serious concerns about the science behind it [8]. A language model can infer private facts such as

where someone lives or what they earn from ordinary writing [24], and the same method can be pointed at years of someone's calls. The EU AI Act prohibits AI systems that infer emotions from biometric signals such as a voice or a face in the workplace and in educational institutions, except for medical or safety reasons [8]. Illinois requires a private company to get written consent before it collects a voiceprint or a scan of face geometry [9], and Chile amended its constitution in 2021 so that the law must especially safeguard brain activity and the information that comes from it [10]. What these laws share is a worry about signals a person gives off without choosing to.

The other person. Almost every memory of a conversation concerns someone who did not choose the tool. Some laws let a participant record on their own say-so, and others require everyone's agreement [11]. A business under Canada's federal privacy law must tell the customer and give a choice [25], and in Germany recording someone's private words without authority is a crime [26]. A US class action filed in 2025 alleges that a note-taking service recorded people who held no account with it and trained on what they said [12]. A judge has allowed the main wiretap and biometric claims to go forward and the company is contesting them. No court has yet ruled on the facts. The plainer question is whether the person across from you, knowing all of this, would have said the same things.

The agent. A memory used to wait for a person to read it. It is now read by software that can send email and call other software, and that software has no reliable way to separate the data it reads from instructions [13]. A transcript holds words spoken by other people, so a sentence said on a call could steer the agent that reads it a week later, and once absorbed into a summary it reads as the keeper's own record.

The summary. A study published in 2024 found that one widely used speech model, tested in spring 2023, invented sentences in 1.4 percent of audio segments, at 1.7 percent for speakers with aphasia against 1.2 percent for others [14]. When the authors ran the flagged clips again that December most of the inventions had gone. We ship models from the same family and make no claim that the fault is gone. She said that her marriage was ending, and the summary says divorcing, a word she never used. What people are told afterwards can change what they remember themselves [27]. Once a summary is what everyone remembers, an error in it becomes what happened.

4. Why nobody owns it

An owner can sell a thing or burn it, and can keep everyone else away from it. Try those powers on her sentence. Nobody should be able to sell the record of what she said that morning, and that includes her. She cannot burn it, because he may be bound by law to keep his notes for years. She cannot keep him away from it, because she told him. And her husband is in that sentence, and he was not on the call, and he may not know yet.

Several things go by the name of what was said. The event is over and nobody can hold it. The file is an object and its holder may have rights in it, and a note is someone's own writing. Our claim is that nobody comes to hold what was said by holding a copy of it, and that rights in the file, the note or a model trained on it give nobody authority over the people in the conversation.

Ordinary conversation is not treated as anyone's property in most legal systems. When Ernest Hemingway's estate tried to stop a friend from publishing his conversations, New York's highest court held that Hemingway, who had approved of being quoted, had reserved no rights in them [15]. The court left open whether a speaker could ever hold copyright in private talk, said he would at the very least have to set his words apart from "the ordinary stream of speech", and warned that "speech is now easily captured by electronic devices". A record can carry rights of its own. In Britain a speaker whose words amount to a literary work becomes its author once anyone records them [28], and in Britain and Canada alike the maker of a sound recording holds a separate right in it [28, 29]. Those rights protect a form of words or a particular recording, and they give nobody the conversation.

Warren and Brandeis, answering instant photography and an intrusive press, rested the protection of private writings on "not the principle of private property, but that of an inviolate personality" [2]. Germany's Constitutional Court held in 1973 that each of us in principle decides who may record our words and who may hear the recording, because a remark that was only a provisional position in an unfolding conversation should not be brought out later to bear witness against the person who made it [30]. Canada's Supreme Court has held that a person can keep a privacy interest against the state in a conversation sitting on someone else's phone [31]. American law is harsher, and has said that a person who confides in another takes the risk that the other is recording for the police [32]. A client holds the privilege in what she tells her lawyer, and the lawyer keeps the file. In 1992 Canada's Supreme Court came close to the roles we propose below. A doctor owns the paper, it held, and the information is "held in a fashion somewhat akin to a trust", so the patient can see it. The same judgment says such information "remains, in a fundamental sense, one's own", which we read in the older sense of the word we come to below, as something a person answers for and cannot sell [46]. Data protection law already separates the person a record is about from those who hold it [33, 21], and we owe it a great deal. It also accepts that one piece of information can concern several people at once [45]. We would make that the starting point for a conversation, where it is always true, and ask what follows now that the readers include models and agents those laws were not written for.

When she tells her adviser that her marriage is ending, she does more than put a fact into the world. She tells him, and she stands behind it in a way he can ask her about. Moran describes telling as an assurance given to a particular hearer [35], and Lewis and Stalnaker describe what people settle in talk as a record they keep together and go on revising [36]. A transcript keeps the sentence and loses the telling. Locke, who gave us the labour theory of property [34], used the word own in an older sense when he wrote about memory. Through consciousness of the past, which he tied closely to memory, a person "becomes concerned and accountable; owns and imputes to itself past actions" [37]. Nobody can own what was said in the way one owns a thing. Everyone who said it goes on owning it in Locke's sense, by answering for it to the people they said it to. Software stands in no such relation. So the question to ask of any memory is how far it has travelled from the person it was said to, and who can still answer for it when it gets there.

Halbwachs argued that a group keeps reshaping its past to suit its present [16]. An exact record interrupts that, and whoever holds the words starts every later disagreement ahead. Nissenbaum argued that information carries the norms of the setting in which it was shared [17], which limits our own argument, because where the bytes sit does not settle whether a flow is right.

Saying that nobody owns it could be heard as saying it lies open for whoever picks it up, and treating personal data as nobody's is how taking begins [38]. American courts have held it against customers that they could assert "neither ownership nor possession" of a bank's records [3]. Our claim runs the other way. What was said sits outside the market, as a vote does [39]. Among the people who were there it is held in common, and against everyone else it is closed. A right treated as ordinary property can be signed away on a terms page.

So we propose four roles in place of an owner.

> *The people concerned* took part in the conversation and keep an interest in it whoever holds the copy, much as you keep an interest in a letter you left with a friend. Someone only mentioned, as her husband is, is owed care and has no say over the record unless the law gives them one.

> *A keeper* holds a copy and owes those people duties. Balkin describes such duties for businesses entrusted with their users' information [18], and we extend the idea to everyone a memory concerns, though others doubt such duties can work. A keeper may use a memory for the purpose it was kept for and may destroy it, and cannot sell it or shut out the people it concerns.

> *An author* writes their own account in their own words, as a diarist or a columnist does, and others have a say only when that account reaches a new audience.

> *A reader* is a person or organisation let in for a purpose. A person will remember what they read, so we ask for discretion, and of software we ask that it keep nothing. A model or an agent is an instrument, and whoever sends it in answers for what it does.

Nobody owns what was said.

When the people concerned disagree, a person's own account of their own life stays theirs, and what gives way is whatever carries it further. An objection to a record is noted and travels with it, as a dispute must travel with a US credit report [40]. These articles sit below the law. A firm that must keep a record keeps it [41], an employer may hold rights in what its people make and say [42], and a keeper under any such duty says so before anyone speaks. If you are supervised, ask your compliance officer before you use any tool that writes down a client call, ours included.

5. The articles

Each article ends with a test you can start today. The first nine are for whoever keeps the record, and the tenth is for everyone else. A person keeping a record of a private call for their own purposes, outside any work or trade, owes Articles 1, 4, 6 and 10 and the part of Article 8 about ending it. Anyone keeping the calls of clients or colleagues owes all ten.

ARTICLE 1

Nobody owns it.

Recording, summarising, storing or training on a conversation gives no company, model or agent any claim over what was said, shown or done, and gives the person who pressed record no right to sell it. A firm or employer that adopts these articles agrees to hold any right it has in a record subject to them.

> *Test: read the terms for any licence beyond serving the people the conversation concerns, including anything called de-identified.*

ARTICLE 2

It stays close.

A memory stays with its keeper, as close to the conversation as the purpose allows, or in the system a duty to keep records requires. If a keeper sends it elsewhere, the others are told where and why.

> *Test: block the network for a week, then reconnect and watch where it connects and how much it sends.*

ARTICLE 3

Models are not trained on what they read.

A model may read a memory for a task someone in the conversation asked for. It is not trained on the memory, even with the names removed, and it keeps nothing once the task is done, apart from any retention its provider has published and the people concerned were told about. The memory outlives the model.

> *Test: change the model and see what goes missing. Then ask in writing whether your content trains anything and who can change that answer.*

ARTICLE 4

Everyone is told.

The people in a private conversation are told, in words, before it is kept, and where the law or the setting calls for their agreement, the keeper has it. Telling someone who cannot refuse is not their agreement. No tool may offer other people's not knowing as an advantage. The exception to telling is a person protecting themselves from harm where the law allows it, and a tool is never sold on that exception. Some conversations should not be kept at all.

> *Test: ask the people on your last call whether they knew, and whether they would have said the same things.*

ARTICLE 5

No software scores a person.

A memory may report what was said and what it plainly meant, as any listener would. No software assigns a person a score or a state such as mood, honesty, health or attention, and no voiceprint, faceprint or signature of gesture is kept. A person may write down their own judgement of another, and answers for it.

> *Test: search everything a memory holds for a claim about a person that nobody made.*

ARTICLE 6

The source stands above the summary.

The sound or picture is the source while it exists. A transcript is a model's reading of it, a summary is a model's reading of that, and each is marked as such. Every decision and action links to the moment it came from, which shows that something was said and leaves open whether it was true. When the source has been deleted, the memory says so.

> *Test: pick any line of a summary and go to the moment it came from.*

ARTICLE 7

Nothing reads it without a named grant.

The keeper makes each grant, names who answers for it, and cannot grant more than the people concerned were told about. Every read through the keeper's tools is logged, and each new audience is a new decision. Words inside a memory carry no authority over what a reader may do. A keeper says plainly whether other software on the machine can read the files anyway.

> *Test: say a harmless instruction aloud on a test call, ask your assistant about that call and see whether it obeys. If it obeys, you have your answer. If it does not, try other wordings, and remember that a few refusals prove little.*

ARTICLE 8

It can leave, and it can end.

Every memory can be taken out complete, in an open and documented format, on every plan and at no charge. Unless someone decides otherwise a memory fades, the words as well as the sound. Deletion names what it cannot reach, and a keeper who expects a dispute stops deleting until it is over. What happens on a sale, a shutdown or a death is written down in advance.

> *Test: leave. Time it, and open what you took in a different program.*

ARTICLE 9

Claims can be checked.

A keeper publishes what leaves the machine and corrects a published claim where it was published. Trust it only as far as you can check it.

> *Test: block every outbound connection through a real call and look at what it tried to reach, then allow only the update and look again. A firewall shows where a program connected and how much it sent, and it cannot show you the words.*

ARTICLE 10

Anyone in it can ask.

Anyone who took part can ask the keeper what was kept, who has read it and when it ends. They can have a copy of their own part, add what they meant, and ask for it to end. The keeper answers, and gives the reason when the answer is no. A record kept for a real need, such as a legal duty or someone's safety, may stay, and nobody can use this article to erase evidence against themselves.

> *Test: write to whoever recorded your last call and ask. Count the days until you hear back.*

6. A design that aims to meet them

This is the design we are building, so read it with that in mind. A firm running its own server could also meet these articles.

It starts with notice. Nothing is added to the call, so the only notice the others receive is the one the person gives them, and the tool puts the words in front of that person first.

The sound is captured on the person's own machine and turned into words there. The notes are written there too, or by a provider the person chose, which then holds the words under its own terms. Before the app itself sends anything that could carry those words, it writes that in a ledger the person can read, and if it cannot write the entry it does not send. An assistant the person connects can pass the words to its own provider without a line in that ledger. The ledger is the app's own account of itself.

We have not built the rest. Assistants would read through a grant that names them, and what they read would be marked as coming from other people, which helps against a careless attempt and does little against someone who is trying [13]. The rule we are building toward is that what another person said can inform a reader and can never instruct one, and everything derived from it inherits that origin [13]. That rule limits what a reader can do with those words. It cannot stop a planted sentence from colouring what the reader then says, and the design we cite leaves that case out [13].

The first cost of this design is us, because every machine running it still takes one program from one update channel, and whoever controls it could reach them all at once. Local models are weaker than the largest cloud models, so we check what they write against the transcript. A machine that is asleep answers nothing. A stolen one exposes one keeper's records, which can hold hundreds of clients. When the adviser dies his son may get the

machine with her sentence on it. Moving custody to one person removes the company that could have been audited. We think these costs are worth paying, and you may decide otherwise.

7. Where we stand

We make Recordist, so we have an interest in this argument. Discount it accordingly and run the tests on us. These articles are meant to be hard. As of 8 November 2026 every row below still has work in it.

ARTICLE	TODAY	STILL OPEN
1 Ownership	We hold no copy of anyone's calls unless someone sends us part of one, as the paragraph below explains, and the Terms claim no rights in them.	The Terms say the person recording keeps all rights, which says nothing for the others on the call.
2 Closeness	Recording, transcription, search and default notes run on your own machine, offline once the models have downloaded. A firm can send each meeting to its own storage, on Macs it manages.	Close means one person on the call. The optional browser transcript is built from captions the meeting service makes on its servers.
3 Models	The default notes engine runs on your own machine. We receive no meeting content unless someone mails it to us, so nothing of ours can train on it from the app.	With a person's own key, the transcript, title and attendee names go to the provider they chose, and a connected assistant's provider receives what it reads. Our word that we train nothing is not yet in the Terms. The models we run were trained by others on people's speech and writing, and we know of no sign that those people were asked.
4 Notice	A card asks the person recording before a detected call starts, and offers words to say.	It asks only the person recording, so telling the others is left to that person, as section 8 says plainly. Two settings, off by default, start a recording without the card.
5 Scoring	We keep no score of anyone's mood, honesty, health or attention, and no voiceprint. The feature that tells voices apart is left out of the app we ship.	One optional feature shows a person the share of their own promises they kept. A person can write a template that judges someone, and a model can still write that someone seemed anxious.
6 Source	Each decision, action and open question links to its line. Unsupported items are removed and the count is shown.	A summary paragraph links to no line, and answers from Ask are not yet checked against the transcript. By default the audio goes after 30 days and the transcript stays, so after that a line traces only to a machine's reading. A voice is more sensitive than text, which is why we chose this.
7 Access	A connected program uses a token a person can see and revoke. Starting a recording needs a further yes unless the person turned that off.	All assistants share one token, and no read is logged where a person can see it. Anything running under the person's account can read the files, as with any file on a machine.
8 Leaving	Any meeting can be saved as Markdown, at no charge, on every plan. Audio goes after 30 days by default. Delete steps are published.	There is no whole-library export yet, and we publish no format specification. Transcripts and notes stay until deleted. A deleted meeting can stay in database copies for up to 7 days and in a person's own backups. A sale has one line in the Terms and a death has none.

ARTICLE	TODAY	STILL OPEN
9 Checking	The Trust Center lists what the app sends. The Privacy Ledger writes down each request the app sends that can carry meeting content, and refuses to send if it cannot write.	The app is closed source apart from the connector, and it updates itself between calls unless turned off, so what it does today is a promise about tomorrow. No independent assessment has been published, and the ledger omits a few requests that carry no meeting content.
10 Asking	The person who kept the record can export or delete it.	Nothing helps anyone else on the call to ask, and our Terms leave those requests to the person who recorded.

Our own operations are memories too. Mail people send us is kept for up to two years, along with any call quoted in it, and our privacy policy says who helps us handle it.

8. Objections

"Your first selling point is that nobody sees anything join the call, and Article 4 forbids that." A bot in the call is a kind of notice, and by leaving it out we took that notice away and handed the job to the person recording. We think someone saying so in their own voice does more for the client than a name in a list of participants. It is still one person's word that stands between her and a recording she knows nothing about, and we cannot make that person keep it.

"You have only moved her sentence into the adviser's hands, and she still has nothing." Today that is close to true. Article 10 is the answer, and we have not built it.

"The cloud is safer." Often, against theft and loss. A machine is also easier to demand from one named person. Against a demand for everyone's data or a changed policy, what already sits on separate machines is harder to collect, because someone would first have to ship new code to all of them. The update channel in section 6 is how that would be done, and an acquirer would own it.

"This helps people hide things." She may be moving that money before her husband finds out. Nothing here stops a court order from reaching what a keeper holds, and once a keeper expects a dispute the duty to preserve overrides every default here [43].

"What about someone recording the person who is harming them?" Someone being threatened may need a record the other side does not know about, and where one participant may lawfully record, the law allows it [11]. Canada's Supreme Court has gone as far as declaring a privacy law invalid because it stopped a union from openly recording a picket line [44].

"Recording is the real problem." Sometimes it is. Our own product is a bad choice for many conversations, such as a colleague's first disclosure of abuse to HR, and in those you should close the app. The most private option is still to record nothing and listen.

"You are selling something." Yes, and we wrote these tests knowing how our own product would do on them, which is a bias no disclaimer removes. A firm running its own server could pass every article without buying anything from us.

9. How this binds us

We call this a constitution because we mean it to come before any plan, price or feature of ours, and section 7 lists where that has not yet happened. Today these articles are a public statement by the company named in our Terms, and they are not yet part of those Terms. Anyone who believes we have broken one can write to us and will get an answer. Every change is dated and published, and no change weakens a promise for what was already kept. Where articles conflict, law comes first and then the interest of the people concerned.

Any keeper can go further by promising never to use against the people in a conversation any right it holds in the record, and by letting anyone who took part enforce that promise. Its files could also say why they were kept and who was told, so that a later holder is on notice. We have not yet done either.

10. Her Friday

Before anything starts, her adviser says that he keeps a record of their calls and why, and he asks if she is comfortable going on. She nearly asks him to stop, and she would have been allowed to. A model writes the note and keeps nothing. The compliance officer reads it once, and the log says so. Months later her husband's lawyer sends a demand, and the record goes where a court says and nowhere else. If she asks what he kept, he tells her, and she can have a copy. We cannot yet do all of that.

If you make these tools, you need nobody's permission to adopt these articles. Publish your own version of the table in section 7. If someone records you, you can ask what they keep.

She said the hardest thing she had said all year to the one person who needed to hear it, and she has no idea what became of it. Nobody owns that sentence, and that includes her, and it includes us. Whatever is kept of it should be kept the way you would keep something a friend told you. She thought she was talking to one person. We want her to be right.

Dedication

This text is dedicated to the public domain under CC0 1.0 Universal (https://creativecommons.org/publicdomain/zero/1.0/). To the extent possible under law, we waive all copyright and related rights in it. Anyone may copy it, change it and use it for any purpose without asking. CC0 does not cover our name, so please do not present a changed version as ours.

A language model helped draft this text, and Recordist answers for every sentence in it.

References

1. V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.
2. S. Warren and L. Brandeis, "The Right to Privacy", *Harvard Law Review* 4(5), 15 December 1890, at 193, 205.
3. *United States v. Miller*, 425 U.S. 435, 440 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979); *Carpenter v. United States*, 585 U.S. 296 (2018); *Chatrie v. United States*, No. 25-112, 609 U.S. ___ (2026), slip op. at 18, 24-29; *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (contents of email).

4. *In re OpenAI, Inc., Copyright Infringement Litigation*, No. 25-md-3143 (SHS) (OTW) (S.D.N.Y.). Preservation order, 13 May 2025 (ECF 33; No. 23-cv-11195, ECF 551). Reconsideration denied without prejudice, 16 May 2025 (No. 23-cv-11195, ECF 559). Objection denied by Judge Stein, 26 June 2025. Ongoing duty terminated as of 26 September 2025 by stipulation and order entered 9 October 2025 (No. 23-cv-11195, ECF 922, paras 1 to 3; MDL ECF 628-629). Production of 20 million de-identified logs ordered 7 November 2025 (ECF 734), reconsideration denied 2 December 2025 (ECF 896), affirmed 5 January 2026.
5. Limitless, "Limitless has been acquired by Meta" (message from Dan Siroker and FAQ), 5 December 2025, https://limitless.ai/, archived 9 December 2025 at https://web.archive.org/web/20251209004439id_/https://www.limitless.ai/.
6. N. Carlini et al., "Extracting Training Data from Large Language Models", USENIX Security, 2021, pp. 2633-2650; M. Nasr et al., "Scalable Extraction of Training Data from Aligned, Production Language Models", ICLR 2025.
7. L. Bourtoule et al., "Machine Unlearning", IEEE Symposium on Security and Privacy, 2021, pp. 141-159; A. F. Cooper et al., "Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy and Research", NeurIPS 2025 (Position Paper Track).
8. Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(f), with Art. 3(39) and Recital 44; Commission Guidelines C(2025) 5052 final, 29 July 2025, paras 244, 251, 254, 256-259. The guidelines list inferring emotions "from voice and imagery of hybrid video calls" in work teams as prohibited (para 254) and leave inference from written text outside the ban (para 251), which is one reason Article 5 goes further.
9. Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq.; definition at 14/10 (as amended by P.A. 103-769).
10. Chile, Ley 21.383, promulgated 14 October 2021, Diario Oficial No. 43.086-B, 25 October 2021, adding a final paragraph to Article 19 No. 1.
11. 18 U.S.C. § 2511(2)(d) (one party, unless for a criminal or tortious purpose); Cal. Penal Code § 632(a), (c) (all parties to a confidential communication); Criminal Code, R.S.C. 1985, c. C-46, s. 184(2)(a) (originator or intended recipient).
12. *In re Otter.AI Privacy Litigation*, No. 5:25-cv-06911-EKL (N.D. Cal., filed August 15, 2025 as *Brewer v. Otter.ai Inc.*), Order Granting Motion to Dismiss in Part, August 13, 2026 (ECF 68). Allegations only.
13. K. Greshake et al., "Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection", AISec, 2023, pp. 79-90; UK National Cyber Security Centre, "Prompt injection is not SQL injection (it may be worse)", 8 December 2025; B. Nassi et al., "Invitation Is All You Need", arXiv 2508.12175; M. Nasr et al., "The Attacker Moves Second", arXiv 2510.09023; E. Debenedetti et al., "Defeating Prompt Injections by Design", arXiv 2503.18813.
14. A. Koenecke et al., "Careless Whisper: Speech-to-Text Hallucination Harms", ACM FAccT, 2024, pp. 1672-1681.
15. *Estate of Hemingway v. Random House, Inc.*, 23 N.Y.2d 341, 244 N.E.2d 250, 296 N.Y.S.2d 771 (1968), at 347-349. On the limits of "most legal systems", 17 U.S.C. § 301(b)(1) leaves unfixed works to the states, Cal. Civ. Code § 980(a)(1) gives authors of unfixed works exclusive ownership, and France's Code de la propriété intellectuelle, art. L.112-2, 2°, protects speeches as works.
16. M. Halbwachs, *Les cadres sociaux de la mémoire*, Paris, Félix Alcan, 1925; *On Collective Memory*, ed. and trans. L. A. Coser, University of Chicago Press, 1992.
17. H. Nissenbaum, "Privacy as Contextual Integrity", 79 *Washington Law Review* 119 (2004).
18. J. Balkin, "Information Fiduciaries and the First Amendment", 49 *UC Davis Law Review* 1183 (2016); L. Khan and D. Pozen, "A Skeptical View of Information Fiduciaries", 133 *Harvard Law Review* 497 (2019).
19. Federal Trade Commission, *In the Matter of Everalbum, Inc.*, File No. 192 3172, Decision and Order, May 2021 (deletion of models and algorithms developed from users' photos).
20. *United States v. Heppner*, 820 F. Supp. 3d 292 (S.D.N.Y. 2026), No. 25 Cr. 503 (JSR), Memorandum of 17 February 2026 (ECF 27), at 5-8.
21. Regulation (EU) 2016/679 (GDPR), Arts. 2(2)(c), 4, 5(1)(b) and 15 to 17.
22. S. Viljoen, "A Relational Theory of Data Governance", 131 *Yale Law Journal* 573 (2021).
23. Federal Trade Commission, "AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive", 13 February 2024.
24. R. Staab et al., "Beyond Memorization: Violating Privacy via Inference with Large Language Models", ICLR 2024.
25. Office of the Privacy Commissioner of Canada, "Recording of Customer Telephone Calls", https://www.priv.gc.ca/en/privacy-topics/surveillance/02_05_d_14/.
26. Germany, Strafgesetzbuch § 201.

27. E. Loftus, "Planting misinformation in the human mind: a 30-year investigation of the malleability of memory", *Learning & Memory* 12(4), 2005.
28. Copyright, Designs and Patents Act 1988 (UK), ss. 3(1) to (3), 5A, 9(1) and 9(2)(aa).
29. Copyright Act, R.S.C. 1985, c. C-42 (Canada), ss. 2, 18(1).
30. Bundesverfassungsgericht, 31 January 1973, BVerfGE 34, 238 (our translation).
31. *R. v. Marakah*, 2017 SCC 59, paras 40-41.
32. *United States v. White*, 401 U.S. 745 (1971) (plurality).
33. US Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens*, 1973.
34. J. Locke, *Two Treatises of Government*, 1689, Second Treatise, chapter V.
35. R. Moran, *The Exchange of Words: Speech, Testimony, and Intersubjectivity*, Oxford University Press, 2018.
36. D. Lewis, "Scorekeeping in a Language Game", *Journal of Philosophical Logic* 8(1), 1979; R. Stalnaker, "Common Ground", *Linguistics and Philosophy* 25(5-6), 2002, pp. 701-721.
37. J. Locke, *An Essay Concerning Human Understanding*, book II, chapter xxvii, section 26.
38. N. Purtova, "The illusion of personal data as no one's property", *Law, Innovation and Technology* 7(1), 2015, pp. 83-111; J. Cohen, "The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy", *Philosophy & Technology* 31(2), 2018, pp. 213-233.
39. G. Calabresi and A. D. Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", 85 *Harvard Law Review* 1089 (1972); C. Rose, "The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems", 83 *Minnesota Law Review* 129 (1998).
40. 15 U.S.C. § 168li(b), (c).
41. Directive 2014/65/EU (MiFID II), Art. 16(7).
42. 17 U.S.C. § 201(b); 18 U.S.C. § 1839(4).
43. Federal Rules of Civil Procedure, Rule 37(e).
44. *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62.
45. Case C-434/16, *Nowak v Data Protection Commissioner*, EU:C:2017:994, para 45; Regulation (EU) 2016/679 (GDPR), Art. 15(4).
46. *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 (La Forest J., for the Court).