

The Television Is Listening:

Smart Television Microphones, All-Party Consent, and the Households

Where Reality Testing Failed

Travis Gilly* 🦋 September 2026 (v0.1)

Abstract

For a period now measured in years, patients who believed the television was listening were told that it was not. They were told by clinicians conducting reality testing, the core technique of cognitive therapy for persecutory delusions, and by family members conducting the ordinary work of reassurance. For some households that statement was false. The device did contain microphones; its manufacturer's own voice agreement concedes that a hands-free feature may capture speech on a false wake without notifying anyone; independent researchers have measured the recognition traffic; and a state attorney general has sued, settled, and obtained a consent decree. This Article argues that the resulting harm to that population is not a privacy injury and is not adequately described as distress. It is the corruption of a disconfirmation channel: the treatment mechanism clinicians and families relied on was operating on a premise nobody could verify and that was, for some patients, wrong, and the reassurance itself, delivered into a belief system that resolves ambiguous social information toward threat, became information about the person delivering it. The Article grounds that harm in law. In Illinois and every other all-party consent jurisdiction, the recording is an offense on the statutes' own definitions, the manufacturer is a principal under the Illinois article's definition of one, and the manufacturer's own terms supply the knowledge element by naming wiretapping and eavesdropping law and assigning compliance to the purchaser. Where a public entity requires attendance in a room containing one of these devices, and where a retailer sells one without disclosure, the effects provisions of the Americans with Disabilities Act reach a burden that falls on this population in a manner different and greater than on others. And the self-help remedy, removing the software, is foreclosed by an anticircumvention regime whose privacy exception a defaulted toggle defeats, whose smart television exemption omits the removal clause written for telephones and voice assistants, and whose rulemaking cannot by statute reach the provision doing the foreclosing. Every remedy obtained or enacted to date is a consent remedy. Those are the right answers to the problem the enforcement identified. They are not answers to this one.

Keywords: persecutory delusions; reality testing; behavioural experiments; belief flexibility; therapeutic alliance; smart televisions; voice recognition; eavesdropping statutes; all-party consent; ADA Title II; ADA Title III; DMCA section 1201.

*Travis Gilly is Founder and Executive Director of the Real Safety AI Foundation. ORCID: 0009-0007-2954-6313. Correspondence: t.gilly@ai-literacy-labs.org. The author discloses the use of speech-to-text software (Wispr Flow) and Anthropic's Claude as assistive technology for a diagnosed neurodevelopmental condition. All legal analysis, case synthesis, theoretical framing, doctrinal arguments, and conclusions are solely the author's own.

Contents

I	Introduction	4
A	What This Article Adds	5
II	The Population the Privacy Literature Does Not Count	6
A	What a Persecutory Delusion Is	6
B	How It Is Treated, and What the Treatment Assumes	7
C	Why This Object	7
D	What Happened Instead	9
E	Why This Is Not Distress	10
F	What It Costs	11
G	The Comparative Question	12
III	The Device	13
A	Two Systems, Defined	13
B	Designed Functionality	14
C	What the Manufacturer Concedes in Its Own Agreements	15
D	Vulnerabilities	16
E	Independent Corroboration	17
F	Enforcement Already Underway	19
1	The Judgment, Read Rather Than Announced	21
G	What the Settlements Reach, and What They Do Not	22
H	One State Has Legislated	23
1	What the Definition Covers, and What It Leaves Out	24
2	Two Provisions Worth Borrowing	24
IV	The Eavesdropping Statute	26
A	The Definitions Do the Work	26
B	Who Is the Party	27
1	The Principal Provision	28
C	The Manufacturer Exemption	30
D	Why the Federal Statute Is Not the Battleground	31
E	How Many States, and Which Ones	32
F	Who Can Bring It	33
V	The Government Waiting Room	34
A	The Provisions	35
B	Coverage	36
C	Compelled Presence	36
D	The Settings, and Their Range	37
E	The Modification	38
VI	At the Counter	38
A	What Is Not Being Argued	39
B	The Structure That Produces the Result	39
C	What the Ticketing Rule Shows	40
D	The Modification That Fits	41

VII	The Remedy Congress Wrote and Then Defeated.....	42
A	The Exposure, Stated Precisely.....	43
B	The Exception Congress Wrote	44
C	Why the Safety Valve Cannot Reach This	44
VIII	Conclusion	46

I. Introduction

A patient says the television is listening. For most of the history of that sentence it was false, and the falsity was what made it useful. A clinician could design a behavioural experiment around it, the exercise in which a patient tests a feared belief against what happens, with confidence in the result. A spouse could say no, it is not, and be right. That was the arrangement in an unknown number of households for as long as televisions have been in living rooms, and it stopped being reliable without anyone announcing it.

This Article is about what that did to the people who were relying on it.

The device in the room now contains microphones. Its manufacturer's own agreement states that a hands-free voice feature may misinterpret a word or sound as the wake signal, that when this happens the product may not notify the user of the collection, and that the speech is deleted from the server afterward.¹ Its terms, in a clause repeated verbatim across four separate agreements, provide that the voices of family members, guests, children, and bystanders may be recorded and analyzed, and that obtaining their consent, in compliance with applicable wiretapping, eavesdropping, and privacy laws, is the sole responsibility of whoever bought the television.² Independent researchers have measured the recognition traffic, a state attorney general has sued five manufacturers, this one has consented to a final judgment, and a legislature has made content recognition opt-in.³

None of that reaches the household this Article describes, and the reason is the subject of Part II. Every remedy obtained or enacted so far is a consent remedy: a clearer screen, an unavoidable disclosure, a real opt-out. Those are correct answers to the problem the enforcement identified, which was that consumers were not told. They are not answers to a

1. LG Elecs. Inc., Voice Information Agreement ¶ 1 (last updated Mar. 2024). *See infra* Part III.

2. LG Electronics, Terms of Use §6(d) (Voice Recognition and Privacy Compliance), <https://www.lg.com/us/terms>; LG Elecs. Inc., Viewing Information Agreement ¶ 13; Voice Information Agreement ¶ 8; Interest-Based & Cross-Device Advertising Agreement ¶ 8; Who.Where.What? User Agreement ¶ 10. Whether those terms bind anyone is a question of contract formation that a companion article takes up; nothing in this one depends on the answer.

3. *See infra* Part III.

household in which the difficulty was never that consent was withheld. The difficulty was that the disconfirmation was false, that the person delivering it did not know, and that for a patient whose condition consists in part of resolving ambiguous social information toward threat, a reassurance is not a neutral fact but a datum about the person offering it.

A. What This Article Adds

Three things.

The population. No literature counts it. The literature on smart television data collection measures what is collected and to whom it is sent; the literature on persecutory delusions measures conviction, flexibility, and interpretation. Nobody has asked what happens to reality testing when the reality changes underneath it. Part II describes the mechanism, from the clinical literature on belief inflexibility and interpretation bias, and says what would be measured if anyone looked.

The eavesdropping analysis. Enforcement to date has proceeded on deception theories, which ask whether the buyer was told. Part IV asks whether the recording is lawful at all where everyone present must consent, and argues that the definitional provisions of the all-party statutes reach this conduct on their face, that the statutory category of principal reaches a manufacturer that never touches the device, and that the manufacturer's own clause supplies the knowledge element that provision requires. That analysis matters to Part II directly: the reassurance was not merely false, it concerned conduct that was unlawful.

The disability frame. Parts V and VI take the two settings in which a person with a persecutory-spectrum condition encounters one of these devices without having chosen it, the government waiting room and the retail counter, and locate the obligation in the effects provisions of the Americans with Disabilities Act and the transaction-design duties its regulations already impose. Part VII explains why the obvious self-help remedy is foreclosed, and why the mechanism Congress built to relieve that foreclosure cannot reach the provision doing the foreclosing.

Between the population and the law sits Part III, which sets out what the device does and what has been done about it, separating designed functionality from vulnerability and recording the enforcement and legislation so that a reader knows what has already been tried before this Article proposes anything.

II. The Population the Privacy Literature Does Not Count

Everything that follows this Part could be written without reference to disability. The eavesdropping analysis belongs to every household in an all-party consent state, the waiting-room and retail analyses reach any person the statutes protect, and the copyright analysis belongs to every owner. This Part concerns a population for whom a networked microphone in the living room does something the privacy framework has no vocabulary for, and for whom the injury is neither the loss of privacy nor distress about it. It comes first because it is the reason the rest is written.

A. *What a Persecutory Delusion Is*

Persecutory delusions are, on the leading cognitive account, threat beliefs: unfounded beliefs that harm will come to the self from others, developed against genetic and environmental risk and maintained by an interacting set of processes including worry, low self-confidence, intolerance of anxious affect, reasoning biases, and safety-seeking behaviour.⁴

Among the recurring contents of those beliefs in clinical practice is the conviction that one is being watched and listened to, and that a household device is the instrument.

Two features of the maintaining architecture matter here. Reasoning biases prevent the processing of alternative explanations, and roughly three quarters of patients with delusions do not report any alternative explanation for the events they cite as evidence.⁵ And safety-seeking behaviour has a specific failure mode: because the patient attributes the absence of harm to the

4. Daniel Freeman, *Persecutory Delusions: A Cognitive Perspective on Understanding and Treatment*, 3 *Lancet Psychiatry* 685, 685 (2016).

5. *Id.* at 687.

protective behaviour rather than to the inaccuracy of the threat belief, disconfirmatory evidence is either not received or not processed.⁶

B. How It Is Treated, and What the Treatment Assumes

The treatment for a threat belief is not persuasion. It is testing.

Cognitive therapy for psychosis works through behavioural experiments: the patient generates a prediction from the belief, enters the feared situation with the maintaining factors reduced, and observes what happens. The clinical aim is described as relearning safety.⁷ The associated construct is belief flexibility, defined as a metacognitive process of thinking about one's own beliefs, changing them in light of reflection and evidence, and generating and considering alternatives.⁸

The technique presupposes something the literature does not state because it has not needed to. It presupposes that the world will cooperate. The experiment is designed on the understanding that the feared thing is not happening, so that entering the situation and attending to the result will produce evidence against the belief.

Outside the clinic the same function is performed continuously and informally, by whoever is present. A spouse says the television is not listening. A parent says nobody is recording. That sentence is not idle reassurance; it is the household performing the disconfirmation that treatment depends on.

C. Why This Object

With the belief and its treatment in view, a word about why the television and not some other device, because the answer is not that televisions happen to have microphones.

6. *Id.* at 688.

7. *Id.* at 689–90.

8. Suzanne Ho-wai So, Daniel Freeman & Graham Dunn, *Jumping to Conclusions, a Lack of Belief Flexibility and Delusional Conviction in Psychosis*, 121 J. Abnormal Psychol. 129, 130 (2012).

Persecutory delusions take their content from the surrounding culture.⁹ The instrument of surveillance in a patient's account has moved with technology across the last century, and the television has held a place in that account since televisions entered living rooms. It is the right size, it is always present, it faces the room, it is on when nobody is attending to it, and it is the one object in a house that has always been understood to transmit in one direction only. A belief that it transmits in both directions is a small modification of an ordinary understanding rather than an invention.

That matters for two reasons.

The first is that the belief was, until recently, reliably false, which is what made it useful in treatment. A clinician working with a patient on this content could proceed with confidence, and a family member could too. The belief was a good candidate for a behavioural experiment precisely because everyone knew how the experiment came out.

The second is that the object has now changed while the belief has not. The patient's account of what the television does has been stable for decades. The television's behaviour has not. What was a delusion for as long as televisions were receivers describes, in a subset of households once the sets acquired microphones and network connections, an approximation of the product specification.¹⁰

This Article does not claim that any patient's belief was correct in its particulars. A patient who believes a television is transmitting to a specific person for a specific purpose is not vindicated by learning that a hands-free feature may capture speech on a false wake and delete it from a server afterward. The claim is narrower and it is about the treatment rather than the belief:

9. Freeman, *supra*, at 685–86 (persecutory delusions as threat beliefs developed against genetic and environmental risk, with content shaped by the individual's circumstances).

10. The manufacturer's own agreements date the relevant voice terms to 2024 and describe hands-free capture as a feature of the current product line. LG Elecs. Inc., Voice Information Agreement (last updated Mar. 2024). Reporting places advertising identifiers and recognition on sets several model years older through firmware updates. *See infra* Part III. The Article does not fix a year and does not need one.

the proposition that the clinician and the family were relying on, that the device in the room is not listening, stopped being true, and nobody told them.¹¹

D. What Happened Instead

For a period now measured in years, in an unknown number of households, the sentence was false.

The device did contain microphones.¹² It did capture speech beyond the interval of any command.¹³ It did transcribe that speech to text and write the text where it persisted.¹⁴ It did enumerate the other devices in the home.¹⁵ Whether any given household's unit did any of this on any given day is a question no occupant could answer, and the manufacturer has structured the product so that no occupant can answer it.

The consequence is not that a private conversation was overheard. It is that a disconfirmation channel was corrupted, and the corruption runs in three directions.

It runs backward. Every reality-testing exercise conducted against a belief of this content, over the period the devices were in circulation, was conducted on a premise the clinician had no way to verify and that was, for some patients, wrong. A patient who accepted the disconfirmation and released the belief did so on false information. That is not a completed treatment. It is a coincidence that resembled one.¹⁶

It runs forward. A clinician cannot now conduct the experiment in good faith. The behavioural experiment requires the clinician to be able to say what will be found, and the honest

11. The manufacturer's own agreement concedes that a hands-free voice feature may misinterpret a word or sound as the wake signal, that the product may not notify the user when this happens, and that collection occurs before deletion. LG Elecs. Inc., Voice Information Agreement ¶ 1. *See infra* Part IV.

12. Reported findings, *infra* Part III (built-in microphone, remote microphone, and other connected audio devices remaining capturable after the built-in switch is disabled).

13. *Id.* (capture window remaining open roughly ten to fifteen seconds after a command and longer if speech continued); LG Elecs. Inc., Voice Information Agreement ¶ 1 (false-wake capture without notification).

14. Reported findings, *infra* Part III (plain-text transcripts on a RAM disk surviving reboot).

15. *Id.* (at least thirty-eight devices enumerated, including phones and watches of people who had never used the set).

16. The clinical aim of the behavioural experiment is described as relearning safety through direct experience that the feared outcome does not occur. Freeman, *supra*, at 689–90. An experiment whose premise is false teaches nothing about safety, whatever the patient concludes from it.

answer for a room containing one of these devices is that finding out would require a packet capture and a firmware decompile. There is no version of that available in a fifty-minute session, and there is no version available to a family member at all.¹⁷

And it runs at the person delivering the reassurance. This is the part with no analogue in the privacy literature. Within a framework organized around the possibility that something is being done to the patient, a reassurance is not exogenous evidence weighing against the belief. It is information about the person offering it. Negative interpretation bias in paranoia resolves ambiguous social information toward threat, at a standardized mean difference around one in clinical populations, rising with symptom severity.¹⁸ A spouse who says the television is not listening, and who is later shown to have been wrong, has not merely failed to help. They have supplied the belief system with a datum about themselves, and the datum is accurate.

E. Why This Is Not Distress

Two characterizations should be resisted, and they are the two the existing frameworks will reach for.

The first is that this is a privacy harm suffered more acutely by a sensitive person. It is not. The privacy injury and this injury are separable: they would arrive on different days, from different facts, and be remedied by different things. A person whose recorded conversation is never disclosed to anyone suffers no privacy consequence and the injury described here is complete.¹⁹

The second is that this is emotional distress. Distress is a response to an injury. What is described here is the disabling of a treatment mechanism, and it is measured in the way treatment

17. The measurement study that established the recognition traffic required a black-box audit of network communications across two countries and multiple viewing scenarios. *See infra* Part III (discussing the measurement study's methodology). The reported voice findings required decompiling firmware and inspecting device logs. Reported findings, *infra* Part III.

18. Antonella Trotta, Jung-Woo Kang & Daniel Ståhl, *Interpretation Bias in Paranoia: A Systematic Review and Meta-Analysis*, 9 *Clinical Psychol. Sci.* 3 (2020).

19. The distinction has a doctrinal analogue in the California scheme, which makes actual damages unnecessary to an eavesdropping claim precisely because the injury is the interception rather than any downstream use. Cal. Penal Code §637.2(c); *see infra* Part IV.

failures are measured: in symptom trajectory, in medication changes, in hospitalization, and in the loss of a therapeutic relationship. The reasoning biases that make the disconfirmation necessary are stable, and do not remit as conviction reduces.²⁰ There is accordingly no later point at which the corrupted channel repairs itself.

F. What It Costs

The measure of this harm is not the patient's distress and it is not the manufacturer's data collection. It is the treatment.

Antipsychotic medication is the primary intervention in schizophrenia-spectrum disorders and nonadherence is a principal driver of relapse.²¹ Cognitive therapy for persecutory delusions is the primary psychological intervention, and belief flexibility is the process it works on.²² Both depend on a relationship: adherence is sustained through the people who administer and encourage it, and belief flexibility is developed with a clinician the patient can afford to believe.²³

A disconfirmation that later proves false does not simply fail to help. It transfers information to the belief system about the person who delivered it, and it does so in a population whose interpretation of ambiguous social information is measurably biased toward threat. The

20. So, Freeman & Dunn, *Jumping to Conclusions*, *supra*, at 136.

21. Dawn I. Velligan, Martha Sajatovic, Ainslie Hatch, Pavel Kramata & John P. Docherty, *Why Do Psychiatric Patients Stop Antipsychotic Medication? A Systematic Review of Reasons for Nonadherence to Medication in Patients with Serious Mental Illness*, 11 Patient Preference & Adherence 449, 449 (2017), doi:10.2147/PPA.S124658 (identifying negative attitude toward medication as a mediator of the effects of insight and therapeutic alliance on intentional nonadherence).

22. The largest treatment effects reported for persistent persecutory delusions come from a theoretically driven cognitive programme built on reducing safety behaviours and relearning safety, tested against befriending with the same therapists. Daniel Freeman et al., *Comparison of a Theoretically Driven Cognitive Therapy (the Feeling Safe Programme) with Befriending for the Treatment of Persistent Persecutory Delusions*, 8 Lancet Psychiatry 696 (2021) (Cohen's *d* of -0.86 on delusional conviction at end of treatment).

23. Meta-analytic effect sizes for cognitive behavioural therapy in psychosis are modest and mask heterogeneous outcomes, with some patients benefiting and others possibly harmed; common factors including the therapeutic alliance play an important role in determining outcomes and have been largely neglected by the research. Katherine Newman-Taylor et al., *Cognitive Behavioural Therapy for Psychosis: The End of the Line or Time for a New Approach?*, 96 Psychol. & Psychotherapy: Theory, Res. & Prac. 1 (2023). The Article does not rest on this; it is cited because a reader should know that the treatment mechanism described here is one whose dependence on the alliance the field itself has begun to name.

spouse who said the television was not listening is not neutral afterward. Neither is the clinician who designed the experiment.

There is no measure of that in the literature and this Article does not invent one. What can be said is what would be measured if anyone looked: symptom trajectory following a disclosure, medication changes, hospitalization, and the survival of the therapeutic relationship. Those are the outcomes by which treatment failures are counted, and they are the outcomes the privacy framework does not reach.

G. The Comparative Question

None of this describes a manufacturer treating anyone differently. The microphone is in every unit. The terms are the same terms. The absence of disclosure at the counter is uniform.

That is the point, and the statute anticipates it. The prohibition reaches methods of administration that have the effect of discriminating on the basis of disability, and effect is the operative word.²⁴ The test asks whether a facially neutral policy burdens the plaintiff in a manner different and greater than it burdens others.²⁵

For most households, an undisclosed microphone is a privacy grievance, and a serious one. For the household described in this Part, the same undisclosed microphone converts an object of treatment into a source of evidence, disables the technique used to treat it, and turns the people administering that technique into participants in the belief. Identical treatment producing unequal enjoyment is the situation the effects provision exists to reach.

There is no study of this. The literature on smart television data collection measures what is collected and to whom it is sent.²⁶ The literature on persecutory delusions measures conviction, flexibility, and interpretation, and the trial literature on behavioural experiments measures whether they reduce conviction, not what happens when their premise fails.²⁷ Nobody

24. 42 U.S.C. §12182(b)(1)(D)(i).

25. *Crowder v. Kitagawa*, 81 F.3d 1480, 1484 (9th Cir. 1996).

26. *See infra* Part III (discussing the measurement study and the advocacy report).

27. *See So, Freeman & Dunn, supra*; *Trotta, Kang & Ståhl, supra*. A search of the trial and review literature on behavioural experiments in psychosis, conducted for this Article through the Consensus index in September 2026,

has asked what happens to reality testing when the reality changes underneath it, and the absence of that study is not evidence that nothing happened.

III. The Device

This Part sets out what the product does. Two cautions govern the whole of it.

The first is sourcing. The findings summarized here are drawn from a published investigation conducted with three independent security researchers, and they are reported as findings rather than adopted as established fact.²⁸ Nothing in the legal analysis that follows depends on any single one of them, and where a finding is load-bearing this Article says so.

The second is a distinction the investigation itself draws and that the legal analysis must preserve. Some of what follows is designed functionality, operating as the manufacturer built it. Some of it is vulnerability, exploitable by a third party who is not the manufacturer. They are different legal problems with different defendants, and conflating them is the fastest way to lose the argument.

A. Two Systems, Defined

Two separate systems are at issue and the analysis depends on keeping them apart.

Automatic content recognition identifies what the television is playing. On the manufacturer's own description, the software continuously analyzes audio signals received directly from the soundboard integrated with the television's speakers, converts them to a

returned studies of command hallucinations, virtual reality exposure, safety behaviour reduction, and therapeutic alliance, and none addressing a disconfirmation later shown to be false. *See, e.g.,* Mirjam Berkhof et al., *Relations Between Changes in Safety Behavior, Paranoid Ideations, Cognitive Biases, and Clinical Characteristics of Patients with a Psychotic Disorder over Time*, 264 *Schizophrenia Res.* (2024) (safety behaviours persist delusions by preventing disconfirmation of threat beliefs). The absence is stated as a finding of the search rather than as a proof of absence.

28. Gamers Nexus (Steve Burke), LG smart television investigation, YouTube (Sept. 5–6, 2026) (135 min.), conducted with Level1Techs (Wendell) and the independent researchers publicly identified as Mr. Bruh and U-Turn, following an initial video on July 16, 2026. The exact video title and URL should be recorded with an archival capture before publication. Contemporaneous coverage as of September 7, 2026 includes Malwarebytes, Cyber Security News, Dexerto, Decrypt, and CyberInsider, each summarizing the same findings; this Article cites the investigation directly rather than the coverage. The investigation ran four months after the manufacturer's Texas judgment. *See infra* this Part.

fingerprint, and compares the fingerprint against a reference database; it does not receive any information directly from the microphone on the television or the remote.²⁹ Recognition listens to what the television plays. It does not listen to the room. Its output is viewing data, and it is governed by the Viewing Information Agreement.

Voice recognition listens to the room. It captures speech through the microphones built into the set and the remote, converts it to text through a service partner, and returns a result. Its output is voice information, and it is governed by a separate Voice Information Agreement.³⁰

The enforcement, the legislation, and the measurement study discussed in this Part concern the first system. The clause examined in this Article, and the population described in Part II, concern the second. Where a finding below belongs to one system and not the other, the text says which.

B. Designed Functionality

Automatic content recognition samples what the display shows and what its speakers emit, converts the sample to a fingerprint, and transmits the fingerprint to servers operated by the manufacturer's advertising subsidiary. The investigation observed telemetry endpoints being contacted at intervals ranging from every seventy-five to ninety seconds to every five to ten minutes depending on the source in use; the recognition transmission interval itself was measured separately by the study discussed below.³¹ The investigation reports that recognition continued while the display was used as a monitor over a video input, with no application of the manufacturer's own software running.

Voice capture, once enabled, was reported to continue for roughly ten to fifteen seconds after a command completed, and longer where speech continued. Captured speech was converted to text and written to logs stored on the device, where it survived a reboot and was cleared only

29. LG Elecs. Inc., Viewing Information Agreement (describing Automatic Content Recognition).

30. LG Elecs. Inc., Voice Information Agreement ¶¶ 1–2.

31. The telemetry figures are the investigation's; the recognition transmission figure of roughly fifteen seconds is the measurement study's. *See infra* this Part.

by disconnecting power. A command to delete data was reported to transmit a deletion request to the manufacturer's servers without clearing the local logs.

Microphone range was demonstrated at forty feet, then at approximately sixty to seventy feet, and in some instances around corners. On one occasion the device captured the conversation of two people working behind it while a third used the voice feature, none of them aware of it.

The device enumerated the local network, returning display names, hardware addresses, signal strengths, and internal addresses for at least thirty-eight other devices, including phones and watches belonging to people who had never used the television, and identifying networked thermostats. It also scanned neighboring wireless networks, which permits geolocation without a positioning receiver.

The physical microphone switch was reported to disable the built-in microphone only. Audio remained capturable from the remote control, an attached webcam, the video input, and other connected audio devices.

Advertising identifiers were observed appearing on older units after firmware updates, on at least one set whose owner reported never having accepted any terms.

C. What the Manufacturer Concedes in Its Own Agreements

Before the reported findings, two concessions in the agreements themselves. They matter because nothing in them depends on a researcher's methodology.

The first concession concerns the microphone, and it is the most important sentence located for this Article.

Under the Voice Information Agreement, the manufacturer states that where the product provides a hands-free voice recognition feature, the feature might misinterpret a word or sound as the wake signal; that when this happens the product may not notify the user of such collection; and that it will promptly delete the voice information from the server.³²

32. LG Elecs. Inc., Voice Information Agreement ¶ 1.

Read that against Part IV. The manufacturer concedes that speech is captured without a wake command, that the user is not notified when it happens, and that a deletion follows on the server. It does not say the capture does not occur. It says the capture occurs, unannounced, and is deleted afterward. Whether a recording that is made without notice and then deleted is an interception is a question the eavesdropping statutes answer on their own terms, and it is not answered by the deletion. The clause also speaks only of the server. It says nothing about what the device retains.

The second concession is that the controls are not one control. A user who submits a do-not-sell request is told, in the same agreement, that recognition services will still be active unless the user also turns off a separate toggle.³³ That is the manufacturer's own account of the architecture, and it is more candid than the settlement's disclosure requirement.

Two further terms bear on later Parts. Voice information is retained for six months before deletion or anonymization.³⁴ And one of the four agreements contains a covenant not to reverse engineer or attempt to reverse engineer the service, or to remove or obscure proprietary notices.³⁵ That is a contractual bar sitting on top of the statutory one discussed in Part VII, reaching conduct the statute might not.

D. Vulnerabilities

Separately, researchers reported remote code execution paths, one requiring a single confirmation and another characterized as non-interactive and withheld pending disclosure. With that access, audio was captured while the network cable was disconnected and retrieved after reconnection, and the on-screen indications associated with voice capture were suppressed.

These findings bear on the analysis in two limited ways. They establish that the capability exists in the hardware independent of the manufacturer's software controls, which is relevant to whether a control that operates in software can be said to disable it. And they establish

33. LG Elecs. Inc., Viewing Information Agreement ¶ 11.

34. LG Elecs. Inc., Voice Information Agreement ¶ 7.

35. LG Elecs. Inc., Who.Where.What? User Agreement ¶ 9.

that the device is a general-purpose computer with persistent storage and network access, which is relevant to what a household is bringing into the room. They do not establish that the manufacturer is doing any of it, and this Article does not assert that it is.

E. Independent Corroboration

The investigation described above is journalism, and a law review article should not rest on it alone. It does not have to. The central findings have independent support in the peer-reviewed literature and in enforcement activity.

A team from University College London, the University of California, Davis, and Universidad Carlos III de Madrid conducted a black-box audit of network traffic between recognition clients and manufacturers' servers, published at the 2024 ACM Internet Measurement Conference.³⁶ Its findings are more precise than the press accounts of them, and in one respect they cut against the argument a reader might expect.

Recognition is agnostic to source. Traffic to recognition endpoints was present during linear television and when the set was used as an external display over a video input, at levels well above other scenarios, and absent during third-party streaming applications, which the authors attribute to copyright constraints and provider agreements rather than to restraint.³⁷ The capture and transmission figures resolve the discrepancy in the Texas materials: the manufacturers' documentation gives capture rates of ten and five hundred milliseconds, while observed transmission runs roughly every fifteen seconds and every minute, which the authors

36. Gianluca Anselmi, Yash Vekaria, Alexander D'Souza, Patricia Callejo, Anna Maria Mandalari & Zubair Shafiq, *Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs*, in Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), Nov. 4–6, 2024, Madrid, <https://doi.org/10.1145/3646547.3689013>, preprint available at arXiv:2409.06203; code and data at <https://github.com/SafeNetIoT/ACR>. The study asked whether recognition is agnostic to how a user watches, whether the privacy controls have any effect, and whether behaviour differs between the United Kingdom and the United States.

37. *Id.* §4.1 (quoting Netflix's stated preference that recognition be deactivated during its streaming to preserve the integrity of its subscribers' viewing experiences and maintain sole control over measurement of its viewership). Watching a laptop through a video port is not an evasion of recognition; it is one of the two scenarios in which recognition is most active.

read as batching.³⁸ Login status makes no difference, suggesting reliance on the advertising identifier or network address rather than the account.³⁹ In both countries the manufacturer examined here contacts a single recognition domain operated by its advertising subsidiary.⁴⁰

And the finding that cuts the other way. The privacy controls worked: once opt-out was exercised, there was a complete absence of communication with any recognition endpoint, on both platforms in both countries, and the authors conclude the opt-out mechanisms are working.⁴¹ That is fatal to nothing here. It removes an argument this Article never makes, since nothing depends on the toggle being broken. It sharpens rather than answers the formation questions taken up in the companion article, because a control that works when exercised is worth little if it is enabled by default and reached through roughly forty clicks under an accessibility heading, and the study says nothing about how many people find it. And it leaves Part II untouched: the study measured recognition traffic, not the microphone, and its scenarios include no one in the room.

Two further items belong in the record.

The first is an advocacy report that has functioned as a regulatory filing. On October 7, 2024 the Center for Digital Democracy published a forty-eight page study of connected television surveillance and sent it, the same day, to the Federal Trade Commission, the Federal Communications Commission, the California Attorney General, and the California Privacy Protection Agency, asking each to investigate.⁴² Its framing is that the streaming business has deliberately incorporated the data-surveillance marketing practices that have long undermined

38. *Id.* §4.1. The two figures in the Texas petition and press release are the capture rates of two different manufacturers; neither is the rate at which data leaves the set.

39. *Id.* §4.2.

40. *Id.* §§4.1, 4.3. In the United Kingdom recognition was inactive on the platform's own free channel service; in the United States the same service produced traffic comparable to linear viewing, a caution against generalizing from one jurisdiction.

41. *Id.* §§4.2–4.3.

42. Jeff Chester & Kathryn C. Montgomery, Ctr. for Digital Democracy, *How TV Watches Us: Commercial Surveillance in the Streaming Era* (Oct. 2024), <https://democraticmedia.org/assets/cdd-ctv-report-oct24-1.1.pdf>; *see also* Letter from Ctr. for Digital Democracy to Hon. Rob Bonta, Att'y Gen. of Cal. (Oct. 7, 2024), <https://democraticmedia.org/assets/caagletter10724final.pdf>.

privacy and consumer protection in the older online world of social media, search engines, mobile phones, and video services, and that this transformation took place largely under the radar of policymakers and the public.

This Article uses that report for context rather than for propositions. It is advocacy, its authors say so, and the measurement study above is the better source for what the devices do. It is cited here for a different reason: it establishes that these practices were placed before four regulators in October 2024, more than a year before the enforcement action described below. Whatever else is true, the agencies were told.

The second is the trade history, which the media studies literature has documented and which this Article does not attempt to duplicate.⁴³

F. Enforcement Already Underway

This Article is not written against a background of regulatory silence. The manufacturer whose clause it examines has already been sued over the underlying practice and has already settled.

On December 15, 2025 the Attorney General of Texas filed five petitions in Texas district courts against five television manufacturers.⁴⁴ The petition against the manufacturer examined here pleads one count under the Deceptive Trade Practices Act alleging two violations: misrepresentation, for presenting the viewing information feature as a tailored viewing experience while knowing the recognition software collects granular data for the manufacturer's and its advertising partners' benefit, and failure to disclose, for not telling consumers that proprietary recognition technology is embedded in the set.⁴⁵ The relief sought is civil penalties of up to ten thousand dollars per violation, with up to two hundred fifty thousand dollars more

43. Ramon Lobato, *Automated Content Recognition (ACR), Smart TVs, and Ad-Tech Infrastructure*, Convergence (2025), doi:10.1177/13548565251327885. Cited here for the account of how recognition became an advertising business line rather than a viewing feature; the article is behind a subscription and has not been read for this draft.

44. Press Release, Office of the Tex. Att'y Gen., Attorney General Paxton Sues Five Major TV Companies for Spying on Texans (Dec. 15, 2025). The five petitions are linked from that release.

45. Texas' Original Verified Petition, Application for Temporary and Permanent Injunctions and Request for an Ex Parte Temporary Injunction, State of Texas v. LG Elecs. U.S.A., Inc., Count I, Violations 1–2 (Tex. Dist. Ct. filed Dec. 15, 2025) [hereinafter Texas Petition] (citing Tex. Bus. & Com. Code §17.46(a), (b)(24)). The posted copy carries a Tarrant County caption and a blank cause number; the matter proceeded to judgment in Bell County under Cause No. 25DCV358507, and the filed original should be obtained from that clerk before citation.

where the practice was calculated to acquire or deprive money or property from a consumer sixty-five or older, which the State pleaded as a separate paragraph of fact.⁴⁶

Four allegations in that petition bear on later Parts and come from a sworn public filing rather than from reporting. It names the six agreements a purchaser is presented at setup and alleges that nearly all consumers select all to finish.⁴⁷ It quantifies the asymmetry at one click to opt in and roughly forty clicks across four or more menus to opt out, naming the patterns in the vocabulary of the design literature.⁴⁸ It alleges a capture interval shorter than the press release's.⁴⁹ And it pleads that recognition data captures or infers highly personal attributes, listing among the resulting profile fields political leanings, sexual orientation, health interests, marital status, family composition and age, and religion.⁵⁰

Two of the five have settled. The first settled on February 26, 2026, agreeing to halt collection or processing of viewing data without express consent and to implement clear and conspicuous disclosure and consent screens.⁵¹ The manufacturer examined here consented to a final judgment on May 11, 2026.⁵² Two manufacturers were made subject to temporary

46. Texas Petition, Prayer for Relief & ¶ 82 (citing Tex. Bus. & Com. Code §17.47(c)(1)). Paragraph numbering approximate; confirm against the filed copy.

47. Texas Petition (describing the consent screen: terms of use and privacy policy, a viewing information agreement, a voice information agreement, an interest-based and cross-device advertising agreement, a marketing communications agreement, and one styled Who.Where.What).

48. *Id.* (describing the opt-out path from the home screen through settings, accessibility, support, and privacy and terms, and alleging privacy zuckering and roach motel). The petition also cites the measurement study discussed below at its own footnote 15.

49. *Id.* (alleging a hash saved every ten milliseconds); *cf.* Press Release, *supra* (describing screenshots every five hundred milliseconds). The two figures are the published capture rates of two different manufacturers, and neither is the rate at which data leaves the set. *See infra* this Part.

50. Texas Petition (describing inferred attributes). Health interests appears in that list; nothing in the petition develops it. The petition also serves as notice under the Texas Data Privacy and Security Act with a thirty-day cure, reserving amendment to add claims under that statute. *Id.* n.35 (citing Tex. Bus. & Com. Code §§541.101–.102, 541.154).

51. Press Release, Office of the Tex. Att’y Gen., Attorney General Paxton Secures Major Agreement with Samsung to Ensure that Texans are Protected from Smart TVs Collecting Their Data Without Their Knowledge (Feb. 26, 2026). No monetary penalty was disclosed. The instrument does not appear to have been posted and has not been obtained; the terms stated are the Attorney General’s characterization.

52. Agreed Final Judgment and Permanent Injunction, State of Texas v. LG Elecs. U.S.A., Inc., Cause No. 25DCV358507 (Tex. Dist. Ct., Bell Cnty., 169th Jud. Dist. 2026) [hereinafter Agreed Final Judgment], <https://www.texasattorneygeneral.gov/sites/default/files/images/press/LG.pdf>. Bell County is confirmed as the forum by contemporaneous reporting of the settlement’s submission for approval.

restraining orders early in the litigation on findings of good cause to believe the practices were false, deceptive, or misleading.⁵³ The petitions against the two China-based manufacturers add allegations this Article does not pursue, concerning obligations under Chinese national security law to furnish data on request; they are noted so that silence on them is not mistaken for a view.⁵⁴

1. The Judgment, Read Rather Than Announced

The instrument is more instructive than the announcement of it, in both directions.

Two definitions in it are unusually good and this Article borrows them. Affirmative express consent means a freely given, specific, informed, and unambiguous indication of a consumer's wishes, demonstrated by an affirmative action, following clear and conspicuous disclosure of the data to be collected, the purposes, and a simple and easily located means of withdrawal.⁵⁵ Clear and conspicuous is defined across six requirements, one of which is that in any communication using an interactive electronic medium the disclosure must be unavoidable.⁵⁶

Four limits belong in the same paragraph. The judgment reaches viewing data only, defined as information collected via recognition about household-level viewing behaviors; it does not reach the microphone, voice transcripts, or the enumeration of other devices on the network.⁵⁷ The prescribed disclosure omits the purpose: the required sentence states that the manufacturer will use recognition technology to identify and analyze content on the device, and says nothing about advertising, the advertising subsidiary, or third-party transfer.⁵⁸ The unavoidable pop-up is prospective, applying to model year 2027 and later, so sets already in

53. Reported in contemporaneous coverage of orders against Hisense (Dec. 17, 2025) and Samsung (Jan. 6, 2026), prohibiting collection, use, sharing, disclosure, sale, or transfer of recognition data from Texas consumers. The orders should be obtained from the respective clerks.

54. *See, e.g.*, Texas' Original Verified Petition, State of Texas v. TCL Tech. Grp. Corp. (Tex. Dist. Ct. filed Dec. 15, 2025). Not obtained for this Article.

55. Agreed Final Judgment ¶ 1(g).

56. *Id.* ¶ 1(h)(iii). Unavoidable is the standard the companion article on formation argues was never met at the point of sale.

57. *Id.* ¶ 1(m).

58. *Id.* ¶ 17(a). A consumer who reads it carefully learns that the television will identify what is on the screen. She does not learn why.

households are outside it.⁵⁹ And the injunction expires and automatically terminates five years after its effective date.⁶⁰

Two further features should be stated for accuracy. The judgment recites that nothing in it is an admission of wrongdoing, and that the State recognizes the manufacturer's proactive efforts to implement strong data privacy practices, including measures that exceed industry norms.⁶¹ And the release is broad: on entry the State withdrew a civil investigative demand issued December 2, 2025 and released all claims it brought or could have brought on the covered conduct, including claims under the Texas Data Privacy and Security Act.⁶²

G. What the Settlements Reach, and What They Do Not

Three observations follow, and they shape what remains to be written rather than making it unnecessary.

The first is that the practice has been found sufficiently doubtful that two manufacturers changed it under legal pressure. Nothing in this Article needs to establish that the collection was a good idea, and a reader inclined to think the whole subject overheated has to account for a state enforcer, five complaints, and two settlements.

The second is that the theory pleaded was deception. The action proceeded under a consumer protection statute, on the ground that consumers were not adequately told and did not meaningfully consent. It did not raise the eavesdropping question, which asks whether the recording was lawful rather than whether it was disclosed. And it did not raise the disability question at all. Both remain open, and the settlements do not resolve them.⁶³

59. *Id.* ¶¶ 17–18 (the thirty-day obligation reaches model year 2025 onboarding screens and the website).

60. *Id.* ¶ 4.

61. *Id.* ¶¶ 6, 11, 14. Paragraph 9 stipulates that viewing data has not been and will not be transmitted from the United States to the People's Republic of China, framed as a representation about past and future conduct rather than as a prohibition on something occurring.

62. *Id.* ¶ 29. The alternative theory the petition reserved was released with the rest.

63. Nor did it raise the question whether the terms bound anyone, which a companion article on contract formation takes up.

The third observation is the one that matters most to Part II, and it is not a criticism of the enforcement action.

The remedy obtained is disclosure. A pop-up on the television, a disclosure on the website, and a clear and simple way to opt out. That is a substantial improvement and it will help most households. It is also, precisely, the remedy this Article argues cannot work for the population described in Part II, and for reasons that have nothing to do with how clear or conspicuous the screen is. A patient whose condition consists in part of resistance to disconfirmatory information is not reached by better information. A person who cannot give consent is not reached by a better consent screen. A guest who never sees the television's setup flow is not reached by anything that appears in it.

H. One State Has Legislated

Enforcement is not the only activity. One legislature has acted. What it did is instructive both for what it reaches and for what every summary of it gets wrong.

Kentucky House Bill 692 passed the House ninety-two to nothing and the Senate thirty-eight to nothing, was signed by Governor Beshear on April 13, 2026, and takes effect July 1, 2027.⁶⁴

The bill's official summary, and every secondary account of it located for this Article, states that it includes automatic content recognition data in the definition of sensitive data. The enacted text does something different. The sensitive data definition is left as it stood, still listing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic and biometric data processed to identify a person, data collected from a known child, and precise geolocation.⁶⁵ What the bill adds is a freestanding duty

64. 2026 Ky. Acts ch. 118 (H.B. 692), signed April 13, 2026. Text quoted from the engrossed version, 26 RS HB 692/EN, <https://apps.legislature.ky.gov/reorddocuments/bill/26RS/hb692/bill.pdf>; the chaptered text should be compared against the engrossed version before publication. Sources differ on the sponsor, some naming Representative Josh Branscum and at least one naming Representative Daniel Fister; the bill carried three Republican sponsors and the primary sponsor should be confirmed from the legislative record.

65. H.B. 692 §1 (amending KRS 367.3611(29)).

in the controller-obligations section: a controller shall not collect automatic content recognition data without a consumer's consent.⁶⁶

The difference matters. A sensitive-data classification would have carried the full apparatus that attaches to that category. A standalone consent duty carries only itself. Anyone citing this statute should read the enrolled text rather than the summary.

1. What the Definition Covers, and What It Leaves Out

The defined term is narrower than the practice. Automatic content recognition data means data about a consumer's content viewing history, collected through technology embedded in or operated through a smart television or smart monitor, that identifies in real time the specific content displayed by analyzing audio or video fingerprints, including content received through broadcast, cable, satellite, streaming, or external inputs.⁶⁷

Content viewing history is the object. Ambient audio is not. Nothing in the definition reaches a microphone capturing a conversation in the room, which is the subject of Part IV and the entire subject of the clause examined in this Article.

The definition also carries three exclusions, and two of them are wide enough to matter. It does not include data collected about a consumer's interactions with content provided by the controller's own services, which appears to exempt recognition performed on the manufacturer's own channel service. And it does not include data generated in the course of providing a feature or service requested by a consumer.⁶⁸ A manufacturer that characterizes recognition as generating the recommendations a viewer asked for will litigate inside that exclusion.

2. Two Provisions Worth Borrowing

Two other features of the amended statute bear on arguments made elsewhere in this Article, and neither is specific to televisions.

66. *Id.* §2 (amending KRS 367.3617(1)(f)).

67. *Id.* §1 (amending KRS 367.3611(3)(a)).

68. *Id.* §1 (amending KRS 367.3611(3)(b)).

The first is data minimization, which states in a consumer protection statute a principle the federal unfairness standard reaches by asking whether an injury is outweighed by countervailing benefits. A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed as disclosed to the consumer.⁶⁹

The second is an anti-waiver provision, and it speaks to the allocation in the clause examined in this Article. Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights under the statute's consumer-rights section is deemed contrary to public policy and is void and unenforceable.⁷⁰ A legislature that has just been shown a set of consumer terms wrote a provision voiding contractual waivers of the rights it was creating. That is a judgment about who should bear the risk of terms nobody reads, and it runs opposite to the allocation in the clause this Article examines.

The remedy is consent, defined as a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, which is demanding and would defeat a great deal of what this Part describes.⁷¹ It is obtained from the consumer who configures the device. Because the defined term stops at viewing history, it does not reach the microphone, and for the reasons developed in Part II it does not reach a guest who is never asked or a household for whom the difficulty was never that consent was withheld.

One further feature of the Texas statute concedes the principle this Article extends. The enhanced penalty applies where the practice was calculated to acquire or deprive money or property from a consumer sixty-five or older, at twenty-five times the ordinary amount. That is a legislative judgment that the same conduct produces a different magnitude of harm depending on who it reaches, and that the difference is large enough to price. The judgment is confined to age. This Article argues that a second population sustains a different and larger harm from the same conduct, and that nothing in the current enforcement framework counts it.

69. *Id.* §2 (amending KRS 367.3617(1)(a)).

70. *Id.* §2 (amending KRS 367.3617(2)).

71. H.B. 692 §1 (amending KRS 367.3611(7)).

Everything the enforcement has reached so far proceeded on the theory that consumers were not told. The next Part asks a prior question.

IV. The Eavesdropping Statute

Every state prohibits some form of surreptitious interception. They divide on a single question: whether one party's consent suffices, or whether all parties must consent. Illinois requires all, and this Part uses the Illinois article as the working example, both because it is representative of the all-party jurisdictions and because the manufacturer's clause names eavesdropping law without limiting itself to any state.

The structure of the analysis is unusual. In most disputes about a recording, the contested question is whether the conversation was private or whether consent was given. Here the definitions decide most of it before the argument begins, and the litigable questions turn out to be who used the device and whether the use was surreptitious.

A. *The Definitions Do the Work*

Illinois defines the offense before it defines the terms, and the terms are where the analysis lands.

An eavesdropping device, under the statute, is any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications, whether such conversation or electronic communication is conducted in person, by telephone, or by any other means. The sole carve-out is for devices used for the restoration of the deaf or hard-of-hearing to normal or partial hearing.⁷²

That definition turns on capability, not on design or purpose. A television with a microphone that can hear and record oral conversation is an eavesdropping device within the statutory definition, and nothing in the text asks whether the manufacturer intended it as one. The provision that does ask about design is the possession offense, which requires that the design

72. 720 ILCS 5/14-1(a) (2026).

of the device render it primarily useful for surreptitious overhearing.⁷³ The offenses that matter here, the use offenses, carry no such qualifier. They require only an eavesdropping device, used surreptitiously, to record a private conversation without the consent of all parties.⁷⁴

A private conversation means any oral communication between two or more persons, whether in person or transmitted by wire or other means, when one or more of the parties intended the communication to be of a private nature under circumstances reasonably justifying that expectation. A reasonable expectation includes any expectation recognized by law, including one derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.⁷⁵

Two consequences. A conversation in a private residence is the paradigm case, not a marginal one. And the express inclusion of privilege-derived expectations reaches the clinician on a patient call, the lawyer on a client call, and the household discussing a matter within the marital privilege, each in a room containing the product.

Surreptitious means obtained or made by stealth or deception, or executed through secrecy or concealment.⁷⁶ Whether the capture in any given household is surreptitious is a factual question, and it is the question on which the design decisions documented in Part III bear most directly.

B. Who Is the Party

The offense is committed by a person who uses an eavesdropping device. The statute divides that person into two cases and the division matters.

Where the person is not a party to the private conversation, the offense requires the consent of all of the parties.⁷⁷ Where the person is a party, the offense requires the consent of

73. 720 ILCS 5/14-2(a)(4) (2026).

74. *Id.* §14-2(a)(1)–(2).

75. 720 ILCS 5/14-1(d) (2026).

76. 720 ILCS 5/14-1(g) (2026).

77. 720 ILCS 5/14-2(a)(1) (2026).

all other parties.⁷⁸ A separate provision reaches a person who uses or discloses information he or she knows or reasonably should know was obtained from a private conversation in violation of the article.⁷⁹

A manufacturer receiving transcribed speech from a living room in another state is not a party to the conversation. If it is a person who uses an eavesdropping device within the meaning of the article, it falls under the first case, and the consent it requires is the consent of everyone in the room.

The purchaser is in a different position, and the clause is what puts him there. A resident speaking in his own living room is a party to the conversation. If the operation of a device he bought, powered, connected, and configured constitutes use by him, he falls under the second case, and the consent he requires is the consent of everyone else present. That is precisely the consent the manufacturer's terms instruct him to go and obtain.

Whether an owner uses a device that operates on its own schedule is a real question and this Article does not resolve it. The definitional section defines an eavesdropper as any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the article.⁸⁰ Operates or participates in the operation is broader than operates, and it is not obvious which side of that line a passive owner falls on. The definition does not address a device that operates automatically without a human operator, and no authority located here supplies the answer.

1. The Principal Provision

The article does not stop at the operator, and the provision that reaches past him has not been part of the public discussion of these devices.

A principal is any person who knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or knowingly derives any benefit or

78. *Id.* §14-2(a)(2).

79. *Id.* §14-2(a)(5).

80. *Id.* §14-1(b).

information from the illegal use of an eavesdropping device by another; or directs another to use an eavesdropping device illegally on his or her behalf.⁸¹ An eavesdropper includes a person who acts as a principal.⁸²

The second branch is the one that matters. It does not require the principal to have operated anything. It requires two things: that another person's use of an eavesdropping device was illegal, and that the principal knowingly derived benefit or information from that use.

Apply it. If the operation of the microphone in a household without all-party consent is an illegal use, then a manufacturer that receives the resulting voice transcripts, retains them for six months, and uses them to generate reports and analyses about voice function usage has derived both benefit and information from that use.⁸³ Benefit and information are stated disjunctively, and the manufacturer has taken both.

That leaves knowledge, and the clause supplies it.

A party that writes into its own terms of use that the voices of family members, guests, children, and bystanders may be recorded and analyzed, that obtaining their consent is necessary, and that the necessary consent must be obtained in compliance with applicable wiretapping, eavesdropping, and privacy laws, has stated on the record that it understands the operation to implicate those statutes and to require consent it is not itself obtaining. The clause was drafted to move a compliance burden. Read against the principal provision, it is also an admission of the mental state the provision requires.

Two limits should be stated. The branch is conditional on the underlying use being illegal, which returns to the unresolved question above. And knowingly is a term of art that will be litigated. Neither limit changes the structural point, which is that the article contemplates liability for a party who never touches the device and who profits from what it hears.

81. *Id.* §14-1(c).

82. *Id.* §14-1(b).

83. LG Elecs. Inc., Voice Information Agreement ¶¶ 2, 7. The content recognition stream is a separate function that, on the manufacturer's own description, does not draw on the microphone, *see supra* Part III, and the principal argument here rests on the voice stream alone.

C. The Manufacturer Exemption

The manufacturer's first answer will be that the article exempts it. The exemption exists and its verbs are the answer to it.

It is not unlawful for a manufacturer or a supplier of eavesdropping devices, or a provider of wire or electronic communication services, their agents, employees, contractors, or vendors to manufacture, assemble, sell, or possess an eavesdropping device within the normal course of their business for purposes not contrary to the article.⁸⁴

Manufacture, assemble, sell, possess. The list does not include use, operate, record, transmit, transcribe, store, or analyze. A provision immunizing the making and selling of a device does not by its terms immunize the operation of that device in a purchaser's home after the sale is complete, and the conduct at issue in this Article is operation rather than sale.

The exemption is also conditioned. It applies to conduct within the normal course of business for purposes not contrary to the article. A purpose of capturing speech beyond the interval of a user command, transcribing it, and retaining the transcript is not obviously a purpose consistent with an article whose subject is the surreptitious recording of private conversation, and the conditional language means the exemption does not resolve that question but rather requires it to be answered first.

Two further points belong here for completeness. The provider of wire or electronic communication services clause is drawn from the vocabulary of carriers and network operators, and whether a television manufacturer occupies that role is a question the phrase does not answer. And the possession offense elsewhere in the section, which asks whether a device's design renders it primarily useful for surreptitious overhearing, is the provision on which the manufacturer has its strongest ground.⁸⁵ A television is not primarily useful for eavesdropping. That is a good answer to a charge under the possession provision, and it is not an answer to the use provisions, which contain no comparable limit.

84. 720 ILCS 5/14-2(c) (2026).

85. *Id.* §14-2(a)(4).

D. Why the Federal Statute Is Not the Battleground

The federal wiretap statute sets a floor rather than a ceiling, and its floor is one-party consent. It is not unlawful under the chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties has given prior consent.⁸⁶ A purchaser who consented, and who is himself present, would therefore satisfy the federal exception as to his own conversations.

Two features of the federal statute nonetheless bear on the analysis.

The first is the proviso attached to the consent exception. The exception does not apply where the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.⁸⁷ Federal one-party consent is accordingly not a safe harbor for conduct that constitutes a state offense, which is where an all-party jurisdiction's article does its work.

The second is the reach of the prohibition itself. It extends to a person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, and separately to a person who intentionally discloses or endeavors to disclose the contents of a communication knowing or having reason to know it was obtained through unlawful interception.⁸⁸ Procurement and disclosure are not confined to the person operating the equipment.

Whether a manufacturer receiving data through automated processes is intercepting, using, or disclosing within the meaning of those provisions is not addressed by the statutory text and is not resolved here. What the text does establish is the shape of the map. Federal law leaves the all-party jurisdictions to their own rules, does not immunize a state offense, and reaches beyond the person holding the device.

86. 18 U.S.C. §2511(2)(d) (2026).

87. *Id.*

88. *Id.* §2511(1)(a), (c).

E. How Many States, and Which Ones

The number of all-party jurisdictions is usually given as somewhere between nine and twelve, and the disagreement reflects genuine variation in what the statutes cover rather than carelessness.⁸⁹

Illinois is the working example because its structure is representative. Three others supply features it lacks, and the differences run toward coverage.

Massachusetts turns on secrecy rather than a reasonable expectation of privacy. Interception means to secretly hear or record, or aid another to do so, through an intercepting device, by any person other than one given prior authority by all parties, and the legislative findings state that the secret use of such devices by private individuals must be prohibited.⁹⁰ Its device definition is broader than the Illinois one in a respect the manufacturer will feel: any device capable of transmitting, receiving, amplifying, or recording a wire or oral communication, with carve-outs only for hearing correction and carrier-furnished telephone equipment.⁹¹

Florida reaches the attempt and the procurement. It is an offense to intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, oral, or electronic communication, with interception lawful where all parties have given prior consent.⁹² The endeavor language means the offense does not require that any usable recording result, which matters for a device whose capture is intermittent, downsampled, and converted to

89. Nine states appear on every list consulted: California, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington. Delaware and Nevada appear on most. Connecticut, Michigan, and Oregon are treated inconsistently, generally because their rules differ between telephonic and in-person communication or because judicial construction has departed from the text. The compilations are commercial and none is citable; a survey should cite the statutes directly or the Reporters Committee for Freedom of the Press state guide. Only Illinois, Massachusetts, Florida, and California have been verified for this Article. For a device that records in a room rather than over a line, the telephonic-versus-in-person distinction cuts toward more coverage.

90. Mass. Gen. Laws ch. 272, §99(A), (B)(4) (2026).

91. *Id.* §99(B)(3). A television is not carrier-furnished telephone equipment.

92. Fla. Stat. §934.03(1)(a), (2)(d) (2025).

a fingerprint before transmission; the procurement language reaches a party who arranges the interception without performing it. A general violation is a third-degree felony.⁹³

F. Who Can Bring It

The preceding subsections have established a set of violations without saying who may complain of them, and that omission would be fatal to the practical value of the analysis. The Illinois, Massachusetts, and Florida provisions are criminal. A person whose living room conversation is transcribed and transmitted has no obvious route into court under any of them, and prosecutors have not shown interest in this conduct.

California is the exception, and it is the reason most litigation in this area is filed there.

The prohibition itself is familiar in shape. A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the communication, whether carried on among the parties in one another's presence or by other device, commits an offense.⁹⁴ A confidential communication is one carried on in circumstances reasonably indicating that a party desires it confined to the parties, excluding public gatherings, open proceedings, and any circumstance in which the parties may reasonably expect to be overheard or recorded.⁹⁵ Person is defined to include a corporation and other legal entity, and to exclude an individual known by all parties to be overhearing or recording.⁹⁶ The carve-outs are for public utilities, equipment furnished under a utility tariff, correctional telephone systems, and hearing aids.⁹⁷ A television is none of those.

What distinguishes the California scheme is the remedy. Any person injured by a violation of the chapter may bring an action for the greater of five thousand dollars per violation

93. *Id.* §934.03(4)(a). The misdemeanor grading at (4)(b) is confined to first offenses involving unscrambled radio communications not undertaken for tortious purposes or commercial advantage and does not reach the conduct discussed here.

94. Cal. Penal Code §632(a) (2025).

95. *Id.* §632(c).

96. *Id.* §632(b).

97. *Id.* §632(e)–(f).

or three times actual damages, may seek an injunction in the same action, and is not required to have suffered or been threatened with actual damages as a prerequisite.⁹⁸

Three features of that provision matter to this Article.

The absence of an actual damages requirement removes the obstacle that defeats most privacy claims. A plaintiff whose conversation was transcribed but never disclosed to anyone has no economic loss to plead, and under most theories that ends the case. Here it does not.

The per-violation measure is doing work whose scale depends on facts not established in this Article. If each transmission is a violation, and if the measurement literature's reported intervals are accurate, the multiplier is large. That is a question for a court and for a record; it is noted here because the answer determines whether the remedy is real.

And the statute reaches entities. Person includes a corporation, which is the answer to an argument that a criminal eavesdropping provision was written with individuals in mind.

None of this makes the California route easy. Confidential communication carries its own limitation, and a defendant will argue that a person who accepted terms describing the recording may reasonably expect to be recorded, which is a formation question addressed in the companion article. But it establishes that in at least one all-party jurisdiction the person harmed has a way into court, and that is what Part IV owed the reader.

V. The Government Waiting Room

The analysis to this point has assumed a household. Part V takes up a different setting, in which the person exposed to the device did not buy it, cannot leave, and is required by a public entity to be present.

The displays at issue are not confined to living rooms. They are reported in hospitals, physicians' offices, waiting rooms, conference rooms, and hotels, and in at least one documented

98. *Id.* §637.2(a)–(c).

instance displaying clinical information during a dental visit.⁹⁹ Public entities furnish waiting areas on the same commercial market as everyone else.

A. The Provisions

Three provisions carry the analysis and each is a regulation rather than a construction of the statute, which matters to how they are pleaded.

A public entity may not, directly or through contractual, licensing, or other arrangements, on the basis of disability, afford a qualified individual an opportunity to participate in or benefit from an aid, benefit, or service that is not equal to that afforded others, or provide one that is not as effective in affording equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement as that provided to others.¹⁰⁰

A public entity may not, directly or through contractual or other arrangements, use criteria or methods of administration that have the effect of subjecting qualified individuals with disabilities to discrimination, or that have the purpose or effect of defeating or substantially impairing accomplishment of the objectives of the entity's program with respect to individuals with disabilities.¹⁰¹

And a public entity shall make reasonable modifications in policies, practices, or procedures when necessary to avoid discrimination on the basis of disability, unless it can demonstrate that the modification would fundamentally alter the nature of the service, program, or activity.¹⁰²

Two features of that set deserve emphasis before the application.

The first is that the effects language is express. The methods-of-administration provision asks about effect and not about purpose, and the second clause asks about purpose or effect in the disjunctive. A claimant does not need to establish that anyone intended the result.

99. Reported findings, Part III *supra*.

100. 28 C.F.R. §35.130(b)(1)(ii)–(iii) (2026).

101. *Id.* §35.130(b)(3)(i)–(ii).

102. *Id.* §35.130(b)(7)(i). Note the limitation at (b)(7)(ii): no reasonable modification is required for a person who meets the definition of disability solely under the regarded-as prong.

The second is the objectives clause, which is the one that fits these facts most closely and is the least used. A method of administration is prohibited where it has the effect of substantially impairing accomplishment of the objectives of the entity's program with respect to individuals with disabilities. The objective of a consultative examination is to determine whether a claimant is disabled. A room arrangement that makes it harder for a claimant with a psychiatric disability to complete the examination impairs that objective as to precisely the population the examination exists to assess.

B. Coverage

Title II of the Americans with Disabilities Act reaches public entities, and the statutory definition covers state and local governments and their instrumentalities.¹⁰³ Federal agencies are outside it and are reached instead through Section 504's prohibition on discrimination in programs conducted by executive agencies.¹⁰⁴ That distinction determines the defendant and it is easy to get wrong.

Consider a claimant attending an examination in connection with an application for disability benefits. Initial and reconsideration determinations in that system are made by state agencies operating under agreement with the federal administration, and consultative examinations are arranged through those state agencies.¹⁰⁵ The state agency is a public entity under Title II and a recipient of federal financial assistance under Section 504 at the same time.

C. Compelled Presence

The feature that distinguishes this setting from a retail one is that attendance is not optional. A person may decline to enter a store. A person summoned to an examination, a hearing, a benefits interview, or a supervision appointment may not, and the consequence of non-attendance is administered by the same entity that controls the room.

103. 42 U.S.C. §12131(1).

104. 29 U.S.C. §794(a).

105. 20 C.F.R. §§404.1503(a), 404.1519 (state agency disability determinations and consultative examinations). The regulatory sections should be confirmed current before filing.

In the disability benefits context the consequence is written into the regulations. If a claimant fails or refuses to take part in a consultative examination without a good reason, the agency may find that the claimant is not disabled, and where benefits are already being received, may find that the disability has stopped.¹⁰⁶

The sequence that follows is short. The entity requires attendance. The room contains a device that, for a claimant with a persecutory-spectrum condition, produces the symptom the examination is convened to assess. The claimant cannot remain. The regulation converts not remaining into an adverse determination.

That sequence also solves a remedial problem. Compensatory damages for emotional distress are unavailable in private actions under the Spending Clause statutes, and the Ninth Circuit has extended that holding to Title II while expressly preserving compensatory damages for lost educational opportunities as economic harm.¹⁰⁷ A claim framed in distress terms will not survive. The harm here is not framed in those terms. It is the lost benefit, which is economic, calculable, and outside the bar.

The same regulation contains a second opening. The agency is directed to consider the claimant's physical, mental, educational, and linguistic limitations in deciding whether there was a good reason for failing to appear.¹⁰⁸ That is accommodation language already in the text, which means an administrative path runs alongside the litigation one.

D. The Settings, and Their Range

The consultative examination is the clearest case because the regulation supplies the adverse consequence. It is not the only one.

106. 20 C.F.R. §§404.1518(a), 416.918(a).

107. *Cummings v. Premier Rehab Keller, P.L.L.C.*, 596 U.S. 212, 230 (2022); *Payan v. Los Angeles Cmty. Coll. Dist.*, 169 F.4th 971, 977–79 (9th Cir. Mar. 11, 2026) (No. 24-1809) (Title II defines its rights and remedies as those of the Rehabilitation Act, a Spending Clause statute, so *Cummings* governs; compensatory damages for lost educational opportunities preserved as economic harm). The Eleventh Circuit reached the same conclusion earlier. *A.W. ex rel. J.W. v. Coweta Cnty. Sch. Dist.*, 110 F.4th 1309, 1314 (11th Cir. 2024) (damages for emotional distress are not recoverable under Title II), *as cited in* *Merkel v. Galva CUSD* 224, No. 4:23-cv-04130 (C.D. Ill. Sept. 2, 2026). *Coweta* and *Merkel* have not been independently analyzed for this Article and are cited from a citing decision.

108. 20 C.F.R. §404.1518(a).

A court date, a probation or parole appointment, a child welfare interview, a public defender intake, a state benefits eligibility appointment, a driver licensing appointment, and a public hospital waiting area are all settings in which a state or local entity requires or effectively requires presence in a room it controls. Each has its own consequence for non-attendance, ranging from a bench warrant to a lapsed benefit to a missed appointment recorded as noncompliance.

Two of those settings raise a further problem the article should name but does not resolve. Where the conversation in the room is between a lawyer and a client, or between a clinician and a patient, the expectation of privacy is one the eavesdropping article expressly recognizes, since a reasonable expectation includes any expectation derived from a privilege.¹⁰⁹ A public entity that places a networked microphone in a room where privileged conversation predictably occurs has done something the disability analysis does not fully capture, and it is a separate problem from the one this Part addresses.

E. The Modification

The requested modification is unusually cheap, which matters to the fundamental alteration defense. Disable the microphone. Disconnect the display from the network. Post notice at the entrance. None of those alters the program the entity administers, and the last of them is what the manufacturer's own terms demand of a private purchaser.

VI. At the Counter

Part VI turns to the seller, and to a narrower question than the one usually asked of retailers.

The retailer is unambiguously covered. The statute lists, among private entities considered public accommodations, a bakery, grocery store, clothing store, hardware store, shopping center,

109. 720 ILCS 5/14-1(d) (2026); *see supra* Part IV.

or other sales or rental establishment.¹¹⁰ A national electronics chain is inside that clause and coverage is not litigable.

A. What Is Not Being Argued

Two claims are available and this Article makes neither.

It does not argue that the retailer must stop selling the product. A regulation provides that the public accommodations title does not require a public accommodation to alter its inventory to include accessible or special goods designed for or facilitating use by individuals with disabilities.¹¹¹ Whatever the outer limits of that provision, an obligation to remove merchandise is not a plausible reading of the statute and would be bad policy if it were.

It also does not argue that the retailer may refuse to sell to a customer who discloses a disability. That refusal is the violation, not the remedy. Congress identified overprotective rules and policies as a form of discrimination in the Act's findings, and the Supreme Court has read that finding as directed at refusals to give an even break to classes of disabled people while claiming to act for their own good in reliance on untested and pretextual stereotypes.¹¹²

B. The Structure That Produces the Result

Those two positions, held together, produce the arrangement this Part describes.

A defense premised on risk to the individual is not categorically unavailable under the Act. *Echazabal* sustained a regulation permitting an employer to decline to place a worker at risk to his own health, reasoning in part that the provision addressing threats to others appeared in a list of qualification standards that may include such a requirement, phrasing pointing away from exclusive specification.¹¹³ The public accommodations title is drafted differently: its direct threat provision is a standalone construction clause followed by a definition, and the definition

110. 42 U.S.C. §12181(7)(E).

111. 28 C.F.R. §36.307(a).

112. *Chevron U.S.A. Inc. v. Echazabal*, 536 U.S. 73, 85 (2002) (citing 42 U.S.C. §12101(a)(5)).

113. *Id.* at 80–81.

speaks of significant risk to the health or safety of others.¹¹⁴ The interpretive move that carried *Echazabal* is not available on that text, though the underlying argument has lost once, in the court below.¹¹⁵

Even where such a defense is available, it is conditioned. The regulation *Echazabal* upheld survived because it required a particularized enquiry, a reasonable medical judgment relying on the most current medical knowledge or the best available objective evidence, and an individualized assessment made after considering the imminence of the risk and the severity of the harm.¹¹⁶ What the Court approved was a clinical determination.

A sales floor is not a place where a clinical determination can be made. So the only defense the law offers a seller who would withhold a product for the buyer's own good requires a judgment the seller is not competent to make, and nothing in the same body of law obliges the seller to say anything at all. The solicitous act is unlawful. The silent one is not.

C. What the Ticketing Rule Shows

Before reaching the modification, one feature of the governing regulation is worth drawing out, because it answers an objection about scope.

The general obligation tracks the statute: a public accommodation shall make reasonable modifications in policies, practices, or procedures when necessary to afford goods, services, facilities, privileges, advantages, or accommodations to individuals with disabilities, unless it demonstrates a fundamental alteration.¹¹⁷ The objection to using that provision here is that it is usually understood to be about physical access and about conduct on the premises, not about what a seller tells a buyer.

114. 42 U.S.C. §12182(b)(3).

115. *Echazabal v. Chevron USA, Inc.*, 226 F.3d 1063, 1066–67 (9th Cir. 2000), *rev'd*, 536 U.S. 73 (2002). The Ninth Circuit read the Title I text as confined to threats to others on the principle that expressing one thing excludes another, and held the EEOC's contrary regulation invalid at the first step of *Chevron*; the Supreme Court reversed by upholding the regulation, not by rejecting the textual reading. The decision carries negative treatment for that reason and is cited here only for the textual argument it made and lost.

116. *Echazabal*, 536 U.S. at 86.

117. 28 C.F.R. §36.302(a) (2026). Note the limitation at §36.302(g): no reasonable modification is required for a person meeting the definition of disability solely under the regarded-as prong.

The regulation's own specific applications answer that. Beyond service animals and check-out aisles, it requires a place of lodging to identify and describe accessible features of its rooms in enough detail to permit an individual with a disability to assess independently whether a given room meets their needs.¹¹⁸ And it requires a seller of tickets to ensure that individuals with disabilities have an equal opportunity to purchase accessible seating during the same hours, at the same stages of sale, through the same methods of distribution, and under the same terms and conditions as other patrons.¹¹⁹

Both are disclosure and transaction-design obligations. Neither is about a ramp. The lodging provision in particular requires a seller to supply, before the transaction, information the buyer needs to determine whether the thing being sold will work for them. That is the shape of the obligation this Part identifies, and the regulation already imposes it in a setting where the consequence of not knowing is a room that does not fit rather than a device that records.

D. The Modification That Fits

The obligation this Part identifies is informational and it operates at the point of sale.

Discrimination includes a failure to make reasonable modifications in policies, practices, or procedures when necessary to afford goods and services to individuals with disabilities, unless the entity demonstrates a fundamental alteration.¹²⁰ Running alongside it is the effects provision, which forbids an entity, directly or through contractual or other arrangements, from using standards or criteria or methods of administration that have the effect of discriminating on the basis of disability.¹²¹

The practice is not that a salesperson lied. It is that no part of the transaction discloses, at the counter, that the product contains microphones or that its terms will assign the purchaser a consent-obtaining duty toward everyone who enters the room. Whether those terms bind

118. *Id.* §36.302(e)(1)(ii).

119. *Id.* §36.302(f)(3).

120. 42 U.S.C. §12182(b)(2)(A)(ii).

121. *Id.* §12182(b)(1)(D)(i).

anyone is a formation question this Article does not take up; the point here does not depend on it, because the disclosure obligation attaches to the sale of the device rather than to the enforceability of what arrives with it. A seventeen-year-old working a shift cannot supply that information and should not be expected to. The failure is institutional, and locating it there is what makes it a methods-of-administration claim rather than an accusation against an employee.

The governing test asks whether a facially neutral practice burdens the plaintiff in a manner different and greater than it burdens others.¹²² For most purchasers the missing disclosure costs nothing. For the household in Part II it is the entire purchase decision.

There is a second respect in which the retailer is closer to the conduct than a bare seller. Where the retailer also performs in-home setup as a service, its personnel connect the device to the household network, navigate the agreements, and configure the microphone settings on the customer's behalf. That is not inventory in any sense. It is a service the public accommodation provides, performed in the customer's home, and the analysis of it does not depend on anything in this Part about what happens at the counter.

Section 36.307 does not foreclose this, and its second subsection may assist. A public accommodation shall order accessible or special goods at the request of an individual with disabilities if, in the normal course of its operation, it makes special orders on request for unstocked goods obtainable from a customary supplier.¹²³ Electronics retailers special-order in the normal course. A request that the retailer source a display without networked microphones is closer to a special order than to an alteration of inventory.

VII. The Remedy Congress Wrote and Then Defeated

Section 1201 of Title 17 provides that no person shall circumvent a technological measure that effectively controls access to a work protected under the Copyright Act, and defines circumvention to include avoiding, bypassing, removing, deactivating, or impairing such a

122. See *Crowder v. Kitagawa*, 81 F.3d 1480, 1484 (9th Cir. 1996).

123. 28 C.F.R. §36.307(b).

measure without authority.¹²⁴ The consequence for a television owner is that the obvious self-help remedy, removing the software that collects and transmits, is not merely a warranty problem.

A. The Exposure, Stated Precisely

The version that circulates in public discussion is wrong in a way that understates the difficulty. An individual who disables telemetry on a television he owns faces no criminal exposure, because criminal penalties require that the person act willfully and for purposes of commercial advantage or private financial gain, and he acts for neither.¹²⁵ What reaches him is civil: injunction, impoundment, costs, fees, an order for remedial modification or destruction of the device, and actual damages and profits or statutory damages between two hundred and twenty-five hundred dollars per act of circumvention.¹²⁶

The consequential exposure falls on someone else. The statute separately prohibits trafficking in any technology, product, service, device, or component primarily designed to circumvent an access control, or having only limited commercially significant purpose other than to circumvent one.¹²⁷ The practical result is not that individuals are prosecuted. It is that the ecosystem which would make the remedy available to people who are not security researchers cannot legally form. A sophisticated owner may accept the civil risk and act alone; everyone else needs a tool, and the tool is what the statute exists to prevent.¹²⁸

124. 17 U.S.C. §1201(a)(1)(A), (a)(3)(A) (2026).

125. *Id.* §1204(a). The five-year figure in press accounts belongs to a provision that does not reach him.

126. *Id.* §1203(a)–(c). The innocent-violator provision is discretionary and places the burden on the violator to prove he was not aware and had no reason to believe his acts constituted a violation, *id.* §1203(c)(5)(A), which a consumer who has read the manufacturer's terms will have difficulty carrying.

127. *Id.* §1201(a)(2). A person who builds a tool letting owners disable the collection, or offers the service for a fee, is inside that provision, and if the offering is commercial, inside the criminal provision as well.

128. One of the four agreements adds a contractual layer, covenanting not to reverse engineer the service or remove proprietary notices. LG Elecs. Inc., Who.Where.What? User Agreement ¶ 9.

B. The Exception Congress Wrote

What is less widely noticed is that Congress anticipated this. Subsection (i), titled Protection of Personally Identifying Information, permits circumvention where the measure or the work it protects contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a person seeking access; where in the normal course of operation it does so without conspicuous notice and without providing the capability to prevent or restrict it; where the act of circumvention has the sole effect of identifying and disabling that capability; and where it is carried out solely for that purpose.¹²⁹

The exception fails in exactly the circumstances that produce the problem, at three points. The notice-and-capability clause is conjunctive and forgiving: a manufacturer that buries a toggle several menus deep, sets it to the collecting position by default, and labels it in terms that do not describe what it governs has nonetheless provided a capability to prevent or restrict collection, and the provision asks whether the capability exists, not whether it is usable, discoverable, accurately labeled, or effective.¹³⁰ The online-activities limitation is contestable as applied to what is displayed on a screen, audible in a room, or present on a network. And the sole-effect requirement conditions the exception on no other effect on access to any work, which telemetry entangled with the operating system will not satisfy. Congress wrote a safety valve premised on the assumption that a manufacturer either provides a way to opt out or does not. The design pattern described here occupies the space the drafters did not anticipate: an opt-out that exists, satisfies the statutory text, and is engineered not to be used.

C. Why the Safety Valve Cannot Reach This

The statute's second mechanism is the triennial rulemaking, in which the Librarian of Congress may adopt temporary exemptions for classes of works whose users are adversely affected in their

129. 17 U.S.C. §1201(i)(1).

130. The section does not address whether circumvention to disable data collection is permitted where the user has already been provided a capability to restrict it, which is the open question and the argument.

ability to make noninfringing uses.¹³¹ Two features of that mechanism place this problem outside it.

The first is on the face of the current rule. There is a smart television exemption; it permits circumvention for the sole purpose of enabling interoperability of lawfully obtained applications.¹³² The exemptions on either side of it, for smartphones and portable computing devices and for voice assistant devices, each permit circumvention for interoperability or to permit removal of software from the device.¹³³ The smart television exemption contains no removal clause. An owner may lawfully strip software from the telephone in his pocket and the voice assistant on his counter, and may not lawfully strip it from the television in his living room. The repair exemption does not fill the gap, because it defines maintenance as servicing to make the device work in accordance with its original specifications and repair as restoring it to that state, and recognition and voice capture are part of the original specifications.¹³⁴

The second is structural. The rulemaking cannot exempt anyone from the anti-trafficking provisions. A determination made in the rulemaking may not be used as a defense in any action to enforce any provision of the title other than the paragraph containing the circumvention prohibition itself.¹³⁵ Suppose the Librarian granted, next cycle, an exemption permitting an owner to disable telemetry on a television he owns. It would reach the act of circumvention and

131. 17 U.S.C. §1201(a)(1)(C), (D). The ninth proceeding concluded with a final rule effective October 28, 2024, adopting more than two dozen exemptions that remain in force until October 2027. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 89 Fed. Reg. 85437 (Oct. 28, 2024) (codified at 37 C.F.R. pt. 201) (Docket No. 2023-5).

132. 37 C.F.R. §201.40(b)(10).

133. *Id.* §201.40(b)(9), (b)(11) (emphasis added). A voice assistant device is defined as one designed to take user input primarily by voice and to be installed in a home or office.

134. *Id.* §201.40(b)(15). Removing them is a departure from specification, which is the one thing the exemption is drafted not to cover.

135. 17 U.S.C. §1201(a)(1)(E). The Copyright Office reads that provision as denying it authority to adopt exemptions to the anti-trafficking prohibitions, *see* Register of Copyrights, Section 1201 Rulemaking: Seventh Triennial Proceeding, Recommendation of the Acting Register of Copyrights 5 (Oct. 2018), and the Department of Commerce agency that consults on the proceeding listed among three concerns a lack of clarity about third-party assistance in light of the anti-trafficking provisions, from which the rulemaking provides no exemption. Letter from Nat'l Telecomm. & Info. Admin. to Shira Perlmutter, Register of Copyrights (Sept. 24, 2024), https://www.copyright.gov/1201/2024/2024_NTIA_DMCA_Letter.pdf. The Office recommended a legislative fix nine years ago, proposing discretion to authorize third parties to assist the beneficiaries of exemptions; it has not been enacted. U.S. Copyright Office, Section 1201 of Title 17: A Report of the Register of Copyrights (June 2017).

nothing else. It would not permit anyone to build the tool, distribute it, or perform the service. The owner would be free to do the thing he cannot do, and everyone capable of helping him would remain where they are.

The Librarian herself has said as much. As a regulatory process focused on technological protection measures for copyrighted content, she wrote in the current rule, section 1201 is ill suited to address fundamental policy issues with new technologies; copyright is but one piece in a national framework for ensuring the security, trustworthiness, and reliability of embedded software; and issues such as these extend beyond the reach of section 1201 and may require a broader solution.¹³⁶ The exception Congress wrote fails on its conditions. The mechanism Congress built to supplement it cannot reach the provision that forecloses the remedy. And the party whose conduct produced the problem is not the subject of either.

VIII. Conclusion

The sentence that opened this Article, that the television is listening, was a delusion for as long as televisions were receivers and describes, in a subset of households now, an approximation of the product specification. The belief did not change. The object did. And the people whose job it was to test the belief, clinicians in sessions and family members in living rooms, were not told.

Read against the Illinois eavesdropping article, the recording those households were reassured about is an offense on the statute's own definitions, and the manufacturer that receives the transcripts is a principal on its own clause.¹³⁷ Read against the disability statutes, a public entity that requires attendance in a room containing the device, and a retailer that sells it without disclosure, have adopted methods of administration that burden this population in a manner different and greater than they burden anyone else.¹³⁸ Read against copyright law, the owner

136. 89 Fed. Reg. at 85445–46 (Determination of the Librarian of Congress). The consulting agency endorsed that assessment, writing that after almost twenty-five years and nine rulemakings the process has nearly reached the limits of what can be done under the statute. Nat'l Telecomm. & Info. Admin., *Advancing Innovation in a Software-Enabled World: Decoding the Complex Section 1201 Rulemaking* (Oct. 28, 2024).

137. *See supra* Part IV.

138. *See supra* Parts V–VI.

who wants the device to stop listening is told that the control exists, that it does not reach every microphone, and that the tool he would need to remove the software cannot lawfully be built.¹³⁹

The practice is not unexamined. A state sued, a manufacturer settled, a legislature acted, researchers measured. Every one of those produced a consent remedy, and the instruments are narrower than the announcements: the judgment reaches viewing data and not the microphone, its prescribed disclosure says the television will identify content and not why, its pop-up applies to model year 2027 and later, and it expires in five years.¹⁴⁰ Those are the right remedies for the problem the enforcement found. A consent screen does not reach a guest who never sees it, a child whom the terms name, or a household member whose condition impairs the capacity the screen assumes. And it does not reach the patient in Part II, because the difficulty there was never that the disclosure was unclear.

The measure of this harm is not privacy and it is not distress. It is symptom trajectory after a disclosure, medication changes, hospitalization, and whether the therapeutic relationship survives. Those are how treatment failures are counted, and nobody is counting them.

139. *See supra* Part VII.

140. *See supra* Part III.

References

- Americans with Disabilities Act of 1990, 42 U.S.C. §§12101–12213.
- Anselmi, G., Vekaria, Y., D’Souza, A., Callejo, P., Mandalari, A. M., & Shafiq, Z. (2024). Watching TV with the second-party: A first look at automatic content recognition tracking in smart TVs. *Proceedings of the 2024 ACM Internet Measurement Conference*.
- California Invasion of Privacy Act, Cal. Penal Code §§630–638.
- Chester, J., & Montgomery, K. C. (2024). *How TV watches us: Commercial surveillance in the streaming era*. Center for Digital Democracy.
- Chevron U.S.A. Inc. v. Echazabal, 536 U.S. 73 (2002).
- Cummings v. Premier Rehab Keller, P.L.L.C., 596 U.S. 212 (2022).
- Crowder v. Kitagawa, 81 F.3d 1480 (9th Cir. 1996).
- Digital Millennium Copyright Act, 17 U.S.C. §§1201, 1203, 1204.
- Federal Wiretap Act, 18 U.S.C. §2511.
- Florida Security of Communications Act, Fla. Stat. §934.03.
- Freeman, D., et al. (2021). Comparison of a theoretically driven cognitive therapy (the Feeling Safe Programme) with befriending for the treatment of persistent persecutory delusions. *Lancet Psychiatry*, 8, 696.
- Freeman, D. (2016). Persecutory delusions: A cognitive perspective on understanding and treatment. *Lancet Psychiatry*, 3, 685.
- Illinois Eavesdropping Article, 720 ILCS 5/14-1 to 5/14-9.
- Massachusetts Interception of Wire and Oral Communications Statute, Mass. Gen. Laws ch. 272, §99.
- Newman-Taylor, K., et al. (2023). Cognitive behavioural therapy for psychosis: The end of the line or time for a new approach? *Psychology and Psychotherapy: Theory, Research and Practice*, 96, 1.
- Payan v. Los Angeles Community College District, 169 F.4th 971 (9th Cir. 2026).
- Rehabilitation Act of 1973 §504, 29 U.S.C. §794.
- So, S. H., Freeman, D., & Dunn, G. (2012). Jumping to conclusions, a lack of belief flexibility and delusional conviction in psychosis. *J. Abnormal Psychology*, 121, 129.
- Social Security Administration regulations, 20 C.F.R. §§404.1503, 404.1518, 404.1519, 416.918.
- State of Texas v. LG Electronics U.S.A., Inc., Cause No. 25DCV358507 (Tex. Dist. Ct., Bell Cnty. 2026) (Agreed Final Judgment and Original Verified Petition).
- Title II and Title III regulations, 28 C.F.R. §§35.130, 36.302, 36.307.

Trotta, A., Kang, J.-W., & Ståhl, D. (2020). Interpretation bias in paranoia: A systematic review and meta-analysis. *Clinical Psychological Science*, 9, 3.

Velligan, D. I., Sajatovic, M., Hatch, A., Kramata, P., & Docherty, J. P. (2017). Why do psychiatric patients stop antipsychotic medication? A systematic review of reasons for nonadherence to medication in patients with serious mental illness. *Patient Preference & Adherence*, 11, 449.

U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 89 Fed. Reg. 85437 (Oct. 28, 2024) (codified at 37 C.F.R. pt. 201).

2026 Ky. Acts ch. 118 (H.B. 692).

🎧 🎧