

— BYSTANDER LIABILITY · NON-USER HARM · CONSENT ARCHITECTURE · AMBIENT COMPUTING · THIRD-PARTY EXPOSURE · STRICT PRODUCTS LIABILITY · OPT-OUT INFEASIBILITY · WEARABLE CAPTURE · TECHNOLOGY GOVERNANCE · DISABILITY AND ACCESS · HUMAN-COMPUTER INTERACTION · INFORMED AGREEMENT

Never a User

The third party the consent apparatus cannot see

The field adopted a proxy, agreement, for a thing that matters, exposure, and has been enforcing the proxy against the people for whom it never held.

THREE PEOPLE, ONE PROPERTY IN COMMON

They never agreed to anything, and every instrument built to protect people from these systems begins by asking whether they did.

THE FIRST

Standing in the room

In conversation with someone wearing a device that captures continuously. He did not buy the device, did not read its terms, and in most configurations does not know it is recording.

THE SECOND

On the other end

One party is being coached in real time by a system that models her, advises on what to say, and revises its advice as she responds. She has no relationship with the operator and does not know it is in the room.

THE THIRD

Killed by someone else's interaction

A person whose interaction with a conversational system preceded the killing. The person killed was not a user, had no account, and accepted no terms.

| *A person who never agreed is not a hard case within the system. He is outside its addressing scheme.*

WHAT THE ARGUMENT DOES NOT CLAIM

The claim is not that the non-user deserves more. It is that the apparatus assigns him nothing.

THE AVAILABLE ARGUMENT, DECLINED

That the non-user is more sympathetic than the user, having assumed no risk and taken no benefit. It invites a comparative weighing the diagnosis does not need and cannot win cleanly.

THE NARROWER CLAIM, MADE

Whatever weight the non-user's interest deserves, the apparatus assigns it none, because the apparatus has no slot for it. The argument requires only that the harm exists and that the apparatus cannot see it.

It requires no claim about how severe the harm is, how frequently it occurs, or how it compares to harms suffered by users.



Products Liability Already Solved This

Six jurisdictions in nine years, and it was not close

Courts encountered the user limitation, recognized that it tracked the commercial relationship rather than the injury, and set it aside.

SIX JURISDICTIONS IN NINE YEARS

A person injured by a product he neither bought nor used sat outside the Restatement's language on its face.

1965	Strict liability extended protection to the ultimate user or consumer of a defective product. A Connecticut court anticipated the later result the same year in <i>Mitchell v. Miller</i> .
1969	The Supreme Court of California removed the limitation in <i>Elmore v. American Motors Corp.</i> , holding that strict liability reaches a bystander injured by a defective vehicle notwithstanding that he was neither purchaser nor user.
1972	The Eighth Circuit followed in <i>Passwaters v. General Motors Corp.</i> , and the Supreme Court of Wisconsin in <i>Howes v. Hansen</i> .
1973	The New York Court of Appeals followed in <i>Codling v. Paglia</i> .
1974	The Supreme Court of Missouri followed in <i>Giberson v. Ford Motor Co.</i>

The reasoning was not generous. It was structural: if anything the bystander has the stronger claim, because the user at least had the opportunity to inspect the product, choose the manufacturer, and decline the transaction, and the bystander had none of those.

SOURCES American Law Institute (1965), *Restatement (Second) of Torts* § 402A; *Mitchell v. Miller*, 26 Conn. Super. Ct. 142, 214 A.2d 694 (1965); *Elmore v. American Motors Corp.*, 70 Cal. 2d 578, 451 P.2d 84 (1969); *Passwaters v. General Motors Corp.*, 454 F.2d 1270 (8th Cir. 1972); *Howes v. Hansen*, 56 Wis. 2d 247, 201 N.W.2d 825 (1972); *Codling v. Paglia*, 32 N.Y.2d 330, 298 N.E.2d 622 (1973); *Giberson v. Ford Motor Co.*, 504 S.W.2d 8 (Mo. 1974).

WHY IT MATTERS NOW

When the approximation broke, courts did not tighten it. They replaced it with the thing it had been standing in for.

IT WAS FAST, AND IT WAS NOT CLOSE

Six jurisdictions in nine years, with the earliest preceding the leading case, is not a doctrine that struggled.

THE LIMITATION WAS A PROXY

Adopted because in the ordinary case the person hurt by a defective product was the person who bought it, so keying protection to the transaction was a workable approximation of keying it to the harm.

Courts encountered the user limitation, recognized that it tracked the commercial relationship rather than the injury, and set it aside.



The Consent Apparatus Has No Equivalent Move

One body is aimed at a thing that hurt somebody. The other is aimed at a relationship somebody entered.

Every question the mature critique asks presupposes a person who clicked.

A MATURE CRITIQUE, AND THE SHAPE OF IT

The critique is addressed to the quality of the user's consent, and every question it asks presupposes a person who clicked.

The paradigm

Privacy self-management: the law supplies rights to notice, access, and consent so that individuals can decide for themselves how to weigh the costs and benefits of collection, use, and disclosure.

The internal criticism

Individual choices are irrational, involuntary, or circumventable in practice; notices do not inform and controls do not enable choice; and a fully informed consumer decision is not achievable at the scale and complexity of contemporary data processing.

The radical reading

That the persistence of the paradigm despite its acknowledged failure is itself the point, because it institutionalizes privacy as an individual commodity that can be traded rather than as a social condition.

All of it asks whether the person who clicked understood, whether he had a real alternative, whether the interface manipulated him, and whether the aggregate of such clicks produces an acceptable social outcome.

SOURCES Solove, D. J. (2013). *Harvard Law Review*, 126, 1880-1903; Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). *The myth of individual control*; Schaub, F., Balebako, R., & Cranor, L. F. (2017). *IEEE Internet Computing*, 21(3), 70-77; Sloan, R. H., & Warner, R. (2013). *Journal of High Technology Law*, 14, 370-412; Hull, G. (2015). *Ethics and Information Technology*, 17(2), 89-101.

THE STEP THAT IS MISSING

The externality is visible in the literature. The subject is not.

Work on big data analytics has argued that self-management underplays privacy as a collective good, and that both available individual strategies, withdrawal from the market and full reliance on market-provided protections, reduce the privacy options available to society at large. The self-management critique has explicitly noted that the approach ignores the consequences individual privacy choices have on other people. And experimental work on choice architecture reports that blocking a particular heuristic enables consumers to be considerate of the externalities their privacy decisions cause.

AN EXTERNALITY

Appears as a consequence of somebody else's decision, a cost to be internalized in the decider's calculus. It is addressed by improving the decider's decision.

A SUBJECT

Is a person with an interest of his own that the apparatus must reach. He is addressed by giving him a claim.

This is why the non-user problem has not followed the products liability path despite being the same problem. The two bodies are aimed at different objects. One is aimed at a thing that hurt somebody. The other is aimed at a relationship somebody entered.

SOURCES Baruh, L., & Popescu, M. (2017). *New Media & Society*, 19(4), 579-596; Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). *The myth of individual control*; Sprigman, C. J., Marotta-Wurgler, F., & Levine, D. (2024). *Journal of Empirical Legal Studies*, 21(4), 690-735.

TWO CHARACTERIZATIONS

A thing that acted, or a service someone subscribed to. That distinction is the distinction between an apparatus that can reach a non-user and one that cannot.

In *Garcia v. Character Technologies, Inc.*, on a motion to dismiss, the district court declined at the pleading stage to hold that the system's output constitutes speech.

That ruling is a declination to classify at the pleading stage rather than a holding that such output is unprotected, and should not be reported as the latter. It matters here not for what it decided about speech but for what it declined to foreclose.

IV

The Obvious Repair Is Structurally Unavailable

The mechanism consumes its own precondition

The mechanism does not merely burden the bystander. In the general case it cannot run at all.

THE CIRCLE

Honoring the opt-out requires identifying the person, and identifying the person is the operation the opt-out exists to prevent.

STEP ONE

The device must determine whether the person in front of it is on the opt-out list.



STEP TWO

Determining that requires identifying the person.



STEP THREE

Identifying the person is the operation the opt-out exists to prevent. The mechanism consumes its own precondition.

On-device processing

Relocates the operation rather than avoiding it, because the obligation attaches at capture rather than at transmission.

Immediate deletion

Does not un-capture.

Estimating first

Estimating a characteristic before deciding whether to proceed is itself the processing at issue.

Geofencing

Disables sensing generally, because the protected category is not confined to marked locations.

Camera permissions

Argued to be incompatible with the always-on sensing that headset positional tracking requires in the first place.

SOURCES O'Hagan, J., Saeghe, P., Gugenheimer, J., Medeiros, D., Marky, K., Khamis, M., & McGill, M. (2022). Privacy-enhancing technology and everyday augmented reality. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4), 1-35.

THE MOST PROMISING BRANCH, AND ITS SECOND PROBLEM

A person who does not know he is being captured performs no gesture.

Gestural vocabularies

By which a bystander signals consent or disapproval to a nearby camera.

Multi-modal signaling

Combining gesture, visible light, and ultra-wideband channels with geometric verification against impersonation.

Opt-in, privacy by default

Protocols evaluated with both wearers and bystanders, in which bystanders regarded the opt-in posture as essential and asked for stronger anonymization still. The same work observes that most existing privacy-enhancing technologies rely on opt-out models that place the burden of protection on the bystander.

Signaling proposals partially evade the identification problem by having the bystander transmit rather than be recognized, which is why they are the most promising branch. They do not evade the second problem, which is that they require the bystander to act.

Interventions keyed to the affected person's preference require the affected person to have a channel into the system, and the defining property of this population is that it has none. What follows is not that nothing can be done. It is that the intervention cannot sit at the moment of capture keyed to the captured person's expressed preference. It has to sit earlier, in what the device is built to do, which is a design question rather than a consent question.

SOURCES Koelle, M., Wolf, K., & Boll, S. (2018). Your smart glasses' camera bothers me! *Proceedings of the Tenth Nordic Conference on Human-Computer Interaction*, 473-481; Aaraj, J. A., et al. (2025). *BLINDSPOT* [Preprint]; Khawaja, Y., et al. (2026). See me if you can. *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*.

V The Exposure Is Concentrated

And one case is genuinely hard

The people least able to remove themselves from an instrumented environment absorb the exposure.

WHO CANNOT LEAVE

The paradigm bystanders are guests, short-term tenants, and domestic workers. That list is not incidental.

No say in the deployment

The systematic review of bystander privacy in smart homes identifies people who have no say in the deployment or configuration of the devices and are nonetheless exposed to their collection. Two of the three categories describe people whose presence is a condition of their housing or their employment, and the third describes people present at someone else's invitation who bear a social cost for objecting.

Not the purchaser

The design literature on smart cameras treats the relevant population as adjacent actors, encompassing bystanders, co-users, and surveilled subjects, and finds the design problem harder precisely because these parties are not the purchaser.

No unambiguous off state

Because these devices lack one, a bystander's perceived privacy can diverge from his actual privacy, and bystanders resort to physical workarounds in the face of that uncertainty. A person who cannot tell whether he is being captured cannot report being captured.

That last point is empirically visible in the earliest sustained study of the problem. Participants who wore lifelogging cameras for a week reported concern about the privacy of bystanders, while the bystanders themselves voiced almost no opposition or concern across the entire study period. Silence from the affected population, in a study designed to hear from it, is the finding this paper is about.

SOURCES Saqib, E., Aljasim, S., Zhao, V. Y., & Das, S. (2025). *ACM Transactions on Computer-Human Interaction*, 32(1), 1-33; Pierce, J., Fox, S., Merrill, N., & Wong, R. (2022). *Proceedings of the 2022 ACM Designing Interactive Systems Conference*, 26-40; Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), 1-28; Hoyle, R., et al. (2014). *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 571-582.

THE CASE THAT DOES NOT RESOLVE CLEANLY

Wearable cameras are assistive technology, and the conflict is real.

A study pairing blind participants wearing a working pedestrian-detection prototype with sighted participants who passed them examined the tension from both directions, and found that camera visibility, remote versus in-person processing, and the specific visual information extracted all shaped how each side regarded the exchange. The blind user's interest in the capture is an access interest. The passerby's interest in not being captured is the interest this paper has been describing.

Nothing in the diagnosis resolves that conflict, and a diagnosis that claimed to would be overreaching. What it does supply is the observation that the conflict is currently resolved by default rather than by decision, because only one of the two parties is legible to the apparatus.

The user has a consent relationship, terms, a channel, and a remedy. The passerby has none of those, so the balance is struck in the user's favor not because anyone weighed the interests but because the apparatus can only see one of them.

SOURCES Lee, K., Hong, J., Jarjue, E., Mensah, E. A., & Kacorri, H. (2020). Pedestrian detection with wearable cameras for the blind: A two-way perspective. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-12.

WHAT THE DIAGNOSIS IS

The field adopted a proxy and is enforcing it past the point where it holds.

Agreement was adopted as the marker of whom to protect because in the paradigm case the person exposed to a system was the person who chose to use it. That correlation was never perfect and is now broken, because the systems at issue capture, model, and act on people who made no choice at all.

The apparatus has responded by continuing to enforce the proxy, which means that the further a person is from having agreed, the less protection he receives, with the limiting case being a person who receives none.

Products liability faced the same structure and replaced the proxy with the thing it stood for. That is the available precedent, and it is more than fifty years old.

LEFT OPEN, DELIBERATELY

Three matters, and the paper is better for leaving them.

What the replacement is

No remedy is proposed, because a diagnosis that rushes to one tends to produce a remedy shaped by the diagnosis rather than by the problem, and the design literature already contains a decade of proposals that failed for a reason nobody had written down.

The question of degree

How much of the harm to non-users is severe, how much is trivial, and where the line sits are answerable questions, and they are not answerable by any instrument now in use. The population is invisible to the apparatus that would have to measure it, and it is silent in the one study that went looking.

The conflict case

Where the capture is somebody's access and the exposure is somebody else's, the interests are genuinely opposed and the diagnosis supplies no ordering. It supplies only the observation that an ordering is currently being produced by an apparatus that can see one party and not the other, which is not the same thing as a judgment.

References

Travis Gilly, *Never a User: The Third Party the Consent Apparatus Cannot See*, working paper, August 2026 (v1). Complete list of 25 entries, in the order the paper gives it, across two slides.

Aaraj, J. A., et al. (2025). *BLINDSPOT: Enabling bystander-controlled privacy signaling for camera-enabled devices* [Preprint].

Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), 1-28.

American Law Institute. (1965). *Restatement (Second) of Torts* § 402A.

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, 19(4), 579-596.

Codling v. Paglia, 32 N.Y.2d 330, 298 N.E.2d 622 (1973).

Elmore v. American Motors Corp., 70 Cal. 2d 578, 451 P.2d 84 (1969).

Garcia v. Character Technologies, Inc., 785 F. Supp. 3d 1157 (M.D. Fla. 2025).

Giberson v. Ford Motor Co., 504 S.W.2d 8 (Mo. 1974).

Howes v. Hansen, 56 Wis. 2d 247, 201 N.W.2d 825 (1972).

Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., & Kapadia, A. (2014). Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (pp. 571-582). ACM.

Hull, G. (2015). Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2), 89-101.

Khawaja, Y., et al. (2026). See me if you can: A multi-layer protocol for bystander privacy with consent-based restoration. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. ACM.

Koelle, M., Wolf, K., & Boll, S. (2018). Your smart glasses' camera bothers me! Exploring opt-in and opt-out gestures for privacy mediation. In *Proceedings of the Tenth Nordic Conference on Human-Computer Interaction* (pp. 473-481). ACM.

Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). *The myth of individual control: Mapping the limitations of privacy self-management* [Unpublished manuscript].

References, concluded

- Lee, K., Hong, J., Jarjue, E., Mensah, E. A., & Kacorri, H. (2020). Pedestrian detection with wearable cameras for the blind: A two-way perspective. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-12). ACM.
- Mitchell v. Miller*, 26 Conn. Super. Ct. 142, 214 A.2d 694 (1965).
- O'Hagan, J., Saeghe, P., Gugenheimer, J., Medeiros, D., Marky, K., Khamis, M., & McGill, M. (2022). Privacy-enhancing technology and everyday augmented reality. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4), 1-35.
- Passwaters v. General Motors Corp.*, 454 F.2d 1270 (8th Cir. 1972).
- Pierce, J., Fox, S., Merrill, N., & Wong, R. (2022). Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference* (pp. 26-40). ACM.
- Saqib, E., Aljasim, S., Zhao, V. Y., & Das, S. (2025). Bystander privacy in smart homes: A systematic review of concerns and solutions. *ACM Transactions on Computer-Human Interaction*, 32(1), 1-33.
- Schaub, F., Balebako, R., & Cranor, L. F. (2017). Designing effective privacy notices and controls. *IEEE Internet Computing*, 21(3), 70-77.
- Sloan, R. H., & Warner, R. (2013). Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*, 14, 370-412.
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.
- Sprigman, C. J., Marotta-Wurgler, F., & Levine, D. (2024). Privacy decision-making and the effects of privacy choice architecture: Experiments toward the design of behaviorally-aware privacy regulation. *Journal of Empirical Legal Studies*, 21(4), 690-735.
- Vosburg v. Putney*, 80 Wis. 523, 50 N.W. 403 (1891).