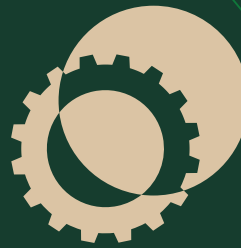


# CONSENT IS DEAD

## HOW CAN WE REVIVE USER-POWERED PERMISSIONS?

EVE MALER, FOUNDER AND PRESIDENT  
22 DECEMBER 2024



# VENN FACTORY

In a keynote at the 2024 European Identity & Cloud conference, I contended that **consent is dead**.

My aim was to stir a thoughtful discussion about the future of digital autonomy and personal data control. I believe the whole notion of user-centric permissions needs a radical makeover if we want it to align with both our privacy ambitions and the harsh realities of data monetization ecosystems.

The digital consent charade is so well known that, over a decade ago, a documentary was made about it: **Terms And Conditions May Apply**. You'd think progress would have been made by now. And yet we're used to seeing headlines like this one: Google and Meta ignored their own rules in secret teen-targeting ad deals.

We've learned of AI cameras detecting passengers' emotions in London, serious privacy critiques of the eIDAS Architecture Reference Framework, and the resurrection of third-party cookies.

**It's time to ditch the checkbox charade and get serious about alternatives.**



Image credit: Internet Safety Labs

# TABLE OF CONTENTS

## Let's Reality-Check the Three Features of Consent • 3

- Consent Feature 1: Manifestation – FAILED • 3
- Consent Feature 2: Knowledge – FAILED • 5
- Consent Feature 3: Voluntariness – FAILED • 7

## Move the Needle by Focusing on New Beliefs • 9

- New Belief 1: Individuals Have the Right to Determine Their Relationship Status • 9
- New Belief 2: Permissions About Digital Assets Should Be Interoperable • 14
- New Belief 3: Data Shielding Requires Potent Solutions • 18

## Personal Data Innovation Scenarios • 24

## Next Steps for Identity Pros • 26

## Privacy Is Context, Control, Choice, and Respect • 30

## About Venn Factory • 30

Venn Factory President and Founder Eve Maler is a Privacy by Design Ambassador and an award-winning standards developer. She has co-founded 7+ standards and contributed to dozens. She owned the identity standards strategy for Sun Microsystems and ForgeRock and owned ForgeRock's patent program.

Eve joined ForgeRock's Office of the CTO in 2014 as it took Series B funding. During her 2020-2023 tenure as ForgeRock CTO, it reached Series E, launched its IPO, and was acquired by Thoma Bravo. With her guiding hand on emerging technology R&D, evangelism, and innovation culture, ForgeRock's ARR rose 85% to \$251.3M, and the company achieved coveted leader status in reports from the top three IAM analysts: Gartner, Forrester, and KuppingerCole.



# Let's Reality-Check the Three Features of Consent

It's easy to suspect **digital consent is a charade**. Just what is broken about this picture?

To be legally binding, consent needs three features. Let's examine the practices surrounding these features and reality-check the limiting beliefs that underlie our current consent approaches.

## Consent Feature 1: Manifestation – FAILED

An **act or manifestation of consent** is the first feature that defines consent. We usually experience this as an “I Agree” button or similar.

**We tell ourselves: We can force data-hungry companies to sip data through a straw.**

On the basis of this belief, enterprises have applied massive and expensive efforts to limit the reach of personal data across the globe, including six solid years of GDPR enforcement and fines.\* Regulators have specified consent requirements in ever greater detail. And as individuals, we all spend more time than ever indicating whether or not we agree to personal data collection, use, and sharing.

**Unfortunately: The identity resolution industry can find us all in a heartbeat.**

Identity resolution is vastly different from identity and access management (IAM):

- **It's indirect.** It's typically handled on the back end by aggregation data processors and other third parties with no direct user relationship.
- **It's heuristic.** It's probabilistic in nature, rather than deterministic, unlike our preferred methods for identity verification and authentication.
- **It uses Big Data.** It uses massive aggregated data lakes and identity graphs to create a 360-degree view of each consumer.



# Thousands of Vendors Focused on Applications, We Operate the Rails

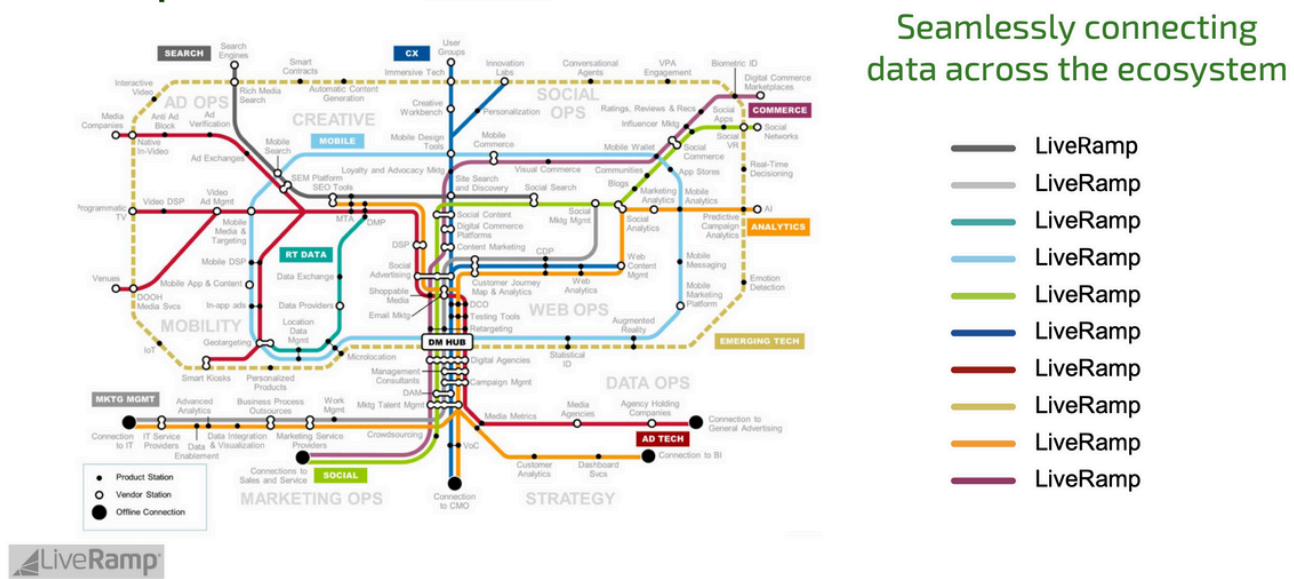


Image credit: [LiveRamp](#)

Few IAM practitioners seem to be aware of this other “identity” industry. It serves as a companion to customer data platforms (CDPs), feeding them answers about who correlates with whom in a unified way to support targeted advertising.

One company in the space, LiveRamp, achieves approximately 100% coverage of the global online population – including the EU – by leveraging cross-links between a myriad of huge data graphs. A newer effort in the space, Unified ID 2.0, adds OpenID Connect technology, familiar to IAM denizens, but does little to change the picture.

The reality is brutally clear. Whether or not people actually “manifest” consent for personal data use – and I’m a privacy nerd who takes a “default-deny” approach to consent – the identity resolution ecosystem makes sure our every digital move is trackable by third parties.

**Reality check: No, we can’t force companies dependent on data monetization to ingest data in tiny sips.**

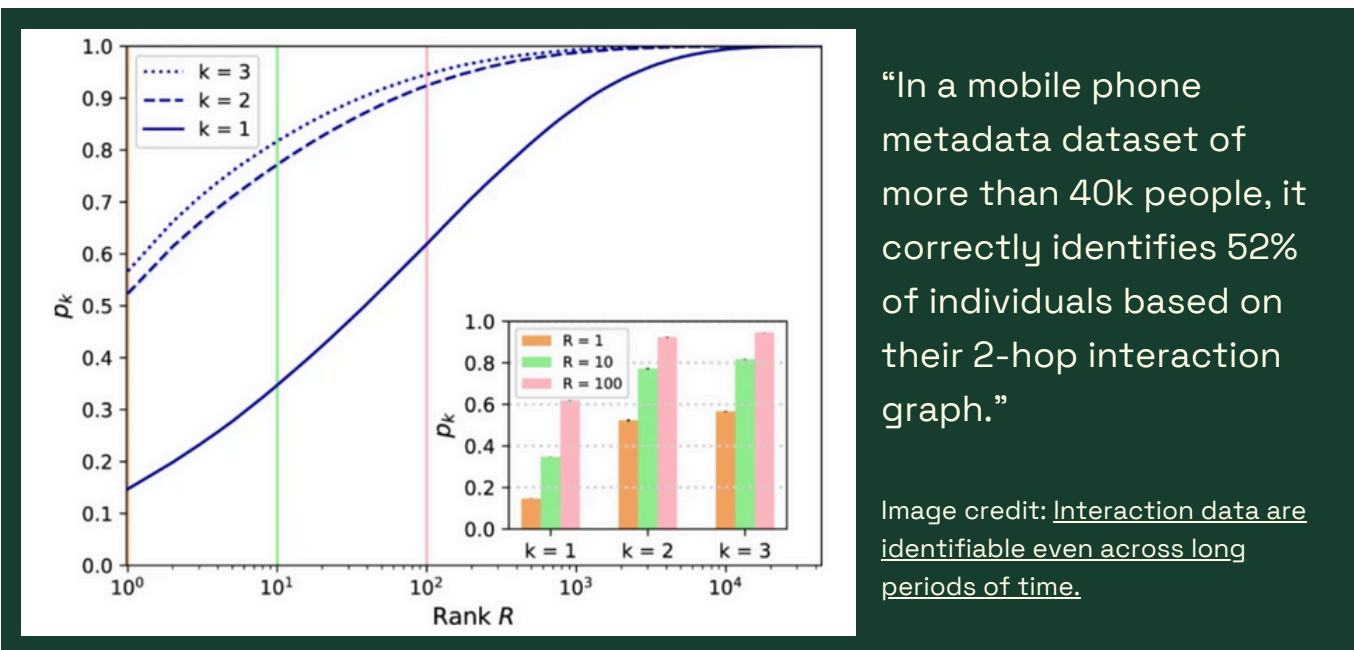
## Consent Feature 2: Knowledge – FAILED

The second feature required for consent to be legally binding is **knowledge**. The aim is to ensure we're sufficiently informed about what we're agreeing to.

**We tell ourselves: We can prevent identity correlation.**

This belief seems logical. If all that personal data is being used so heavily to market to consumers, can't we just stop sharing so much in the first place? Self-sovereign identity (SSI) solutions even offer cryptographic methods like Zero Knowledge Proofs (ZKPs) to help individuals practice selective disclosure in a technically enforceable way. And User-Managed Access has selective sharing at its core.

**Unfortunately: Re-identification is typically a simple operation away, even in the presence of sparsely shared data.**



A profiling attack can successfully re-identify as many as 52% of anonymized social graph members, using only a 2-hop interaction graph and auxiliary data such as the time, duration, and type of a user's interaction with a system – metadata that's effectively impossible not to share.



Anonymization methods are a big part of the problem. The conventional technique used is k-anonymity, where a data set is transformed to remove specificity. Although k-anonymized data is treated and regulated as if it were no longer personal data, it's very easy to crack. Wikipedia says “The guarantees provided by k-anonymity are aspirational, not mathematical.”

Dr. Sam Smith, creator of the Key Event Receipt Infrastructure (KERI) protocol, argues that using k-anonymity constitutes privacy-washing. What's more, he levels a serious charge against the strength of privacy protections that come from user-selected disclosure and the use of ZKP.

The selective disclosure, whether via Zero-Knowledge-Proof (ZKP) or not, of any 1st party data disclosed to a 2nd party may be potentially trivially exploitably correlatable via re-identification correlation techniques.

Selective disclosure is a naive form of K-anonymity performed by the discloser (presenter). The discloser is attempting to de-identify their own data. Unfortunately, such naive de-identified disclosure is not performed with any statistical insight into the ability of the verifier (receiver) to re-identify the selectively disclosed attributes.

– Sustainable Privacy, Samuel M. Smith, September 15, 2023

What's worse, selective disclosure contexts give a false impression of data safety and privacy while encouraging the sharing of verifiably true information. It's a double whammy, and the individual has little chance of understanding – being knowledgeable about – the “exhaust data” left behind from their online activities, making re-identification easy.

**Reality check: No, we can't prevent identity correlation using conventional techniques.**

Even using stronger anonymity techniques such as differential privacy and synthetic data privacy is not without its perils, according to Dr. Smith.

**The individual has little chance of understanding the exhaust data they are shedding, making re-identification easy.**



## Consent Feature 3: Voluntariness – FAILED

The third feature required for consent to be legally binding is **voluntariness**. (Non-lawyers would say “volition.”) We have to be truly willing. A manifestation of consent without either knowledge or voluntariness is considered defective.

**We tell ourselves: We can empower people by asking them something at the point of service.**

A random person asks you to unlock your password-protected smartphone and hand it over for them to search through while you waited in another room.

**What would you do?**

Image credit: [xmlgrl x Ideogram](#)



**Unfortunately: People are easily manipulated into agreeing despite their doubts.**

The “Voluntariness of Voluntary Consent” study published in the Yale Law Journal found that 97% of test subjects acquiesced to unlocking their phones for a stranger.

We may have the best of intentions, but when someone is requesting access, we’re programmed to want to comply. Now imagine it’s a police officer asking for not just your mobile driver’s license but anything else you may have stored in your phone.

You probably suspected that this user-empowerment belief was false already. As identity ethicist Nishant Kaushik puts it:

When denial of consent means denial of service, do people really have a choice?

That's not even counting the ubiquity of actual deceptive patterns or the practice of running consent farms.

There is a structural reason for this. **Consent** is legally asymmetrical; the individual is first approached by the consent seeker. When you're tantalizingly close to getting what you want – whether online or in the real world – the power dynamics are skewed.

**Contract** is another legal structure, also involving consent, for example when we're agreeing to terms of service and privacy policies. It's got a few properties that theoretically provide more symmetry, but in practice we've all witnessed the problem with these contracts of adhesion.

Privacy researcher Daniel Solove recently published an indictment of both opt-in and opt-out consent constructions in these contexts as “fictions of consent.”

**Reality check: No, it's not reasonable to expect to empower people by asking them anything right at the point of service.**

The asymmetry and coercion baked into these interactions mean people don't have true choice.

The purpose of a system is what it does. There is, after all, no point in claiming that the purpose of a system is to do what it constantly fails to do.

– Cybernetician Stafford Beer

**We may have the best of intentions, but when someone is requesting access, we're programmed to want to comply.**





## Move the Needle by Focusing on New Beliefs

Cheer up! Doesn't it feel good to collect knowledge about the defects in today's digital consent systems? It helps us figure out how we can move the needle in creating new, more effective systems.



Let's explore three alternative beliefs that could reshape our approach to digital privacy, personal data rights, and user-centric permissions.

We'll also look at examples of cutting-edge solutions that could help us live up to those beliefs.

### **New Belief 1: Individuals Have the Right to Determine Their Relationship Status**

In human relationships, we generally accept that any one person can decide to call it quits. Research shows that 27% of breakups happen through a phone call and 32% of breakups occur by text message. Why can't we break up with a digital service via a tap?

After all, you lose control over your data with just one or two simple clicks – “I agree” or “Continue.” Even if you reject cookies or say no in other ways, you never know who will get their hands on your data next, painting a digital portrait of you so they can push camping gear ads right after you search for summer vacation spots.

It’s like your data is attending a never-ending party, and you can’t leave or clean up after yourself.

Why can’t we have the same freedom to decide on the status of a relationship in the digital realm?

Instead of being effectively forced to surrender our data forever, we could assume a realistic amount of control – for example, being able to change our minds when we feel a digital relationship with a business isn’t working.

The GDPR notion of a **data subject**, now spreading throughout the regulatory world, empowers individuals somewhat more than its ancestral Data Protection Directive did. But it doesn’t do much to enable a basis for true relationship choice.

If we believe **individuals have the right to determine their relationship status**, we’d probably think about the “subjects of data” differently, and perhaps regulate differently too.

Consider these two potential solutions that could help us live up to this belief. **Lisa LeVasseur**, founder of [Internet Safety Labs\\*](#), and I mooted both in a 2019 [research article](#).

**The GDPR notion of a data subject doesn’t do much to enable a basis for true relationship choice.**



## Relationship Choice Solution: The Me2B Lifecycle Model

The Me2B lifecycle model imports social norms into the digital context using concepts from interpersonal psychology and behavioral economics. It advocates for interactions where the individual (Me) is on an equal footing with the business (B), ensuring that the individual's rights and preferences are respected and prioritized.

In the physical world, there are specific behavioral social norms and expectations for each of these stages of the Me2B Lifecycle. One doesn't expect to be greeted by name, for instance, before any introductions have been made. Similarly, we don't expect store employees to know our home address unless we've given it to them for a specific reason (such as delivery).

- [Internet Safety Labs](#)




As you interact with digital service providers through different stages, their permissions would adapt – and the data they are permitted to know and use may grow, or wane. When you meet a “digital date” for the first time, it should be up to you whether to proceed. You could even decide to end the relationship and get back to “New phone, who dis?” stage with them.

This doesn't mean loyalty programs must come to an end. Individuals and businesses alike could benefit from an uncoerced, transparent, and trustworthy association for such purposes.

Learn more about the complexities of digital relationships in ISL's [Flash Guide #6](#).

## Relationship Choice Solution: Right-to-Use Licensing

The challenges with the **consent** and **consent-to-contract** legal structures highlight how a third structure – a **license** – may help us live up to this new belief.

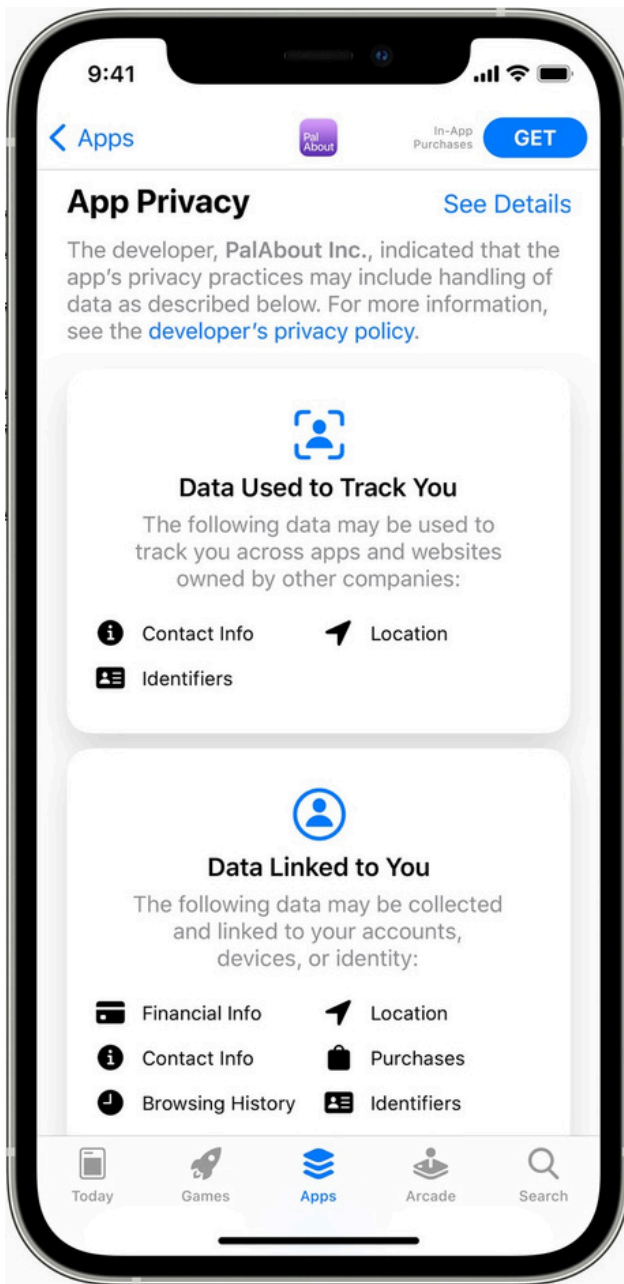
	Consent	Contract	License
Used for?	Opt-in, opt-out	TOS and privacy policy	Right to use my data
Meeting of the minds?	Not required (“pulled”)	Required	Not required (“pushed”)
Revocable?	Unilateral by consenter	Bilateral	Unilateral by issuer
Terms recorded?	No	Yes, in contract	Yes, in license text

Contracts require a “meeting of the minds” to find the intersection of the parties’ common interests. It’s sadly only theoretical with online terms of service and privacy policies, which act as adhesion contracts.

Plain consent is worse because services “pull” your agreement when they ask you to opt in or out. There’s coercion baked right into the experience.

If you could instead license the right to use your data, you’d be “pushing” terms to others, which could remediate the power imbalance. Those terms could cover personal data collection, use, further sharing, and more.

Such power in your hands could be incorporated into services in a seamless fashion. Think of how standardized [Creative Commons](#) licensing is baked into tools such as photo sharing sites.



Privacy nutrition labels such as Apple's are useful for informing you. What if you could inform services of your terms?

Image credit: [Apple](#)

Notice that, while a contract would at least record the terms you “agreed to,” plain consent doesn’t come with this automatically. Right-to-use licensing puts it directly in the license text.

Wouldn’t it be great if personal data usage terms were like [Creative Commons](#) by being human-, machine-, and lawyer-readable?

Most attractively, you can revoke licensed rights in a way that mirrors human relationships.

If you’re not interested to continue, whether because of a trust issue or any other reason at all, you can end things. And you could even calibrate license rights proportionally to the context.

An [IEEE group](#) has been exploring solutions for “Machine Readable Personal Privacy Terms” and a variety of researchers have proposed similar models.

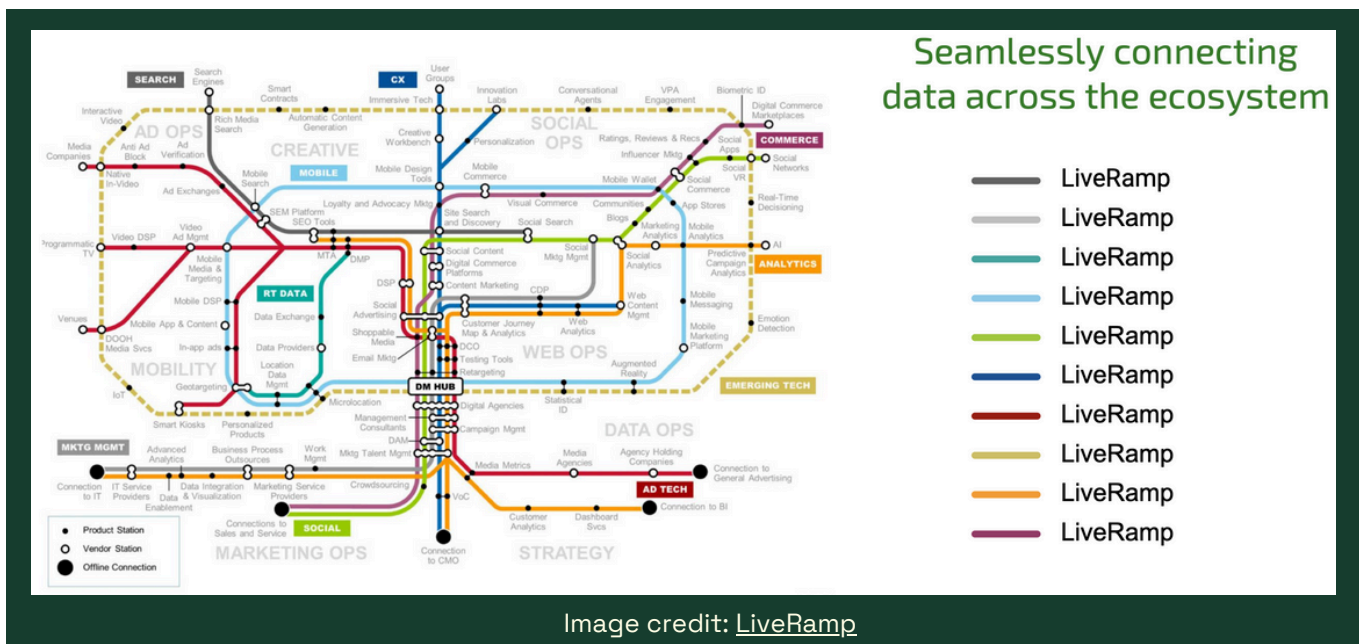
If supported by additional data ecosystem protections, this approach could prove effective.



## New Belief 2: Permissions About Digital Assets Should Be Interoperable

How can we expect the connected world to treat people's wishes as first-class objects without **interoperability**?

If you wanted to visualize services that give you online experiences and serve you ads, it would look like a gigantic transport schematic map. Actually, we don't have to imagine it, because [LiveRamp](#) has helpfully illustrated its "rails" for doing just that.



GDPR doesn't allow data controllers – services with primary responsibility for personal data usage decisions – to give away their **liability** for what happens as a result. But these interactions are a confusing mess and hide a multitude of data sins.

Even the European Commission, in its second report on GDPR results, is calling for more efficiency, consistency, enforcement, and unification to improve access. Meanwhile, new EU laws like the Data Act promote enhanced **business data sharing**.

To enable meaningful individual control of personal data, we need to standardize more of the **back-end interactions** and **artifacts** around data rights and user permissions.

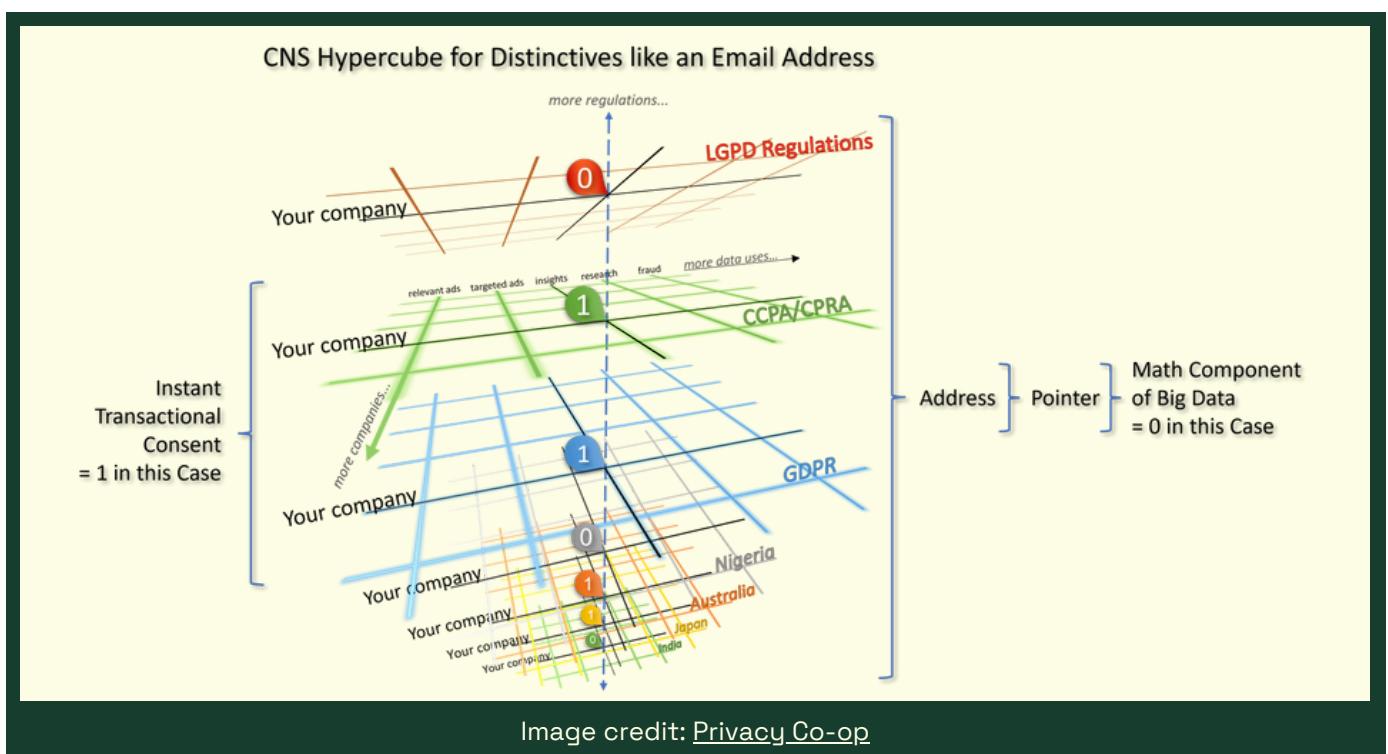
If we believe **permissions about digital assets should be interoperable**, what would the world look like? Maybe we don't have to start with wholesale change. Consider these three solutions that could help boost near-term outcomes in our existing consent-based ecosystem.

## Interoperable Permission Solution: Consent Name System

In the chaos, a business needs to know exactly what data rights it has:

- At **this** moment...
- for **this** purpose...
- given the relevant **legal** jurisdictions...
- and the relevant **business** agreements...
- for **this** person and their individually provided permissions.

It's a tall order. Luckily, we can look to the **Consent Name System (CNS)** to help answer exactly these types of questions.



Innovated by the [Privacy Co-op](#), the CNS is a clever way to deliver – to you as a business stakeholder – a clear and unambiguous answer that you can take to the bank...and to court if necessary.

## Interoperable Permission Solution: Consent Receipts

As already noted, one of the weaknesses of consent as a legal construct is that there's no official record of what it was the person agreed to, unlike with consent-to-contract and right-to-use licensing.

Luckily, the Kantara Initiative has been working diligently on a standard that can capture what was agreed to, in a group called ANCR: Anchored Notice and **Consent Receipts**. (More background is [here](#).)

Think of Consent Receipts as the digital equivalent of shopping receipts, documenting the who, what, when, and why of every consent interaction. These receipts can be easily referenced and audited, providing users and organizations with a clear, verifiable record of all consent transactions.



This transparency could be combined with aggregated tracking mechanisms to hold businesses to greater account than if consent were stored in proprietary systems exclusively on the business side.

The Financial Data Exchange in 2019 agreed to build on Consent Receipts for its financial industry standards efforts, demonstrating an interesting trend in “open banking” models. Consent Receipts have also been imported into standard ISO/IEC 27560 – The Consent Record Information Structure.

**Think of Consent Receipts as the digital equivalent of shopping receipts.**



## Interoperable Permission Solution: Standardized Do-Not-Sell Signal

If a data processor bears ultimate responsibility for correctness of personal data processing, and it involves tens or hundreds of third parties in that processing, shouldn't it have some way to tell all those partners when someone's data is not to be further shared or sold?

Individuals currently can't make their data step off the train before it traverses the entire railway network. This seems like a significant gap in the ability to enforce GDPR and similar laws.

Image credit:  
[RailroadSignals.us](https://RailroadSignals.us)



A recent [Identerati Office Hours](#) session discussed an intriguing possibility for standardizing how the network of services could pass along such a signal: the [Shared Signals Framework](#) (SSF). A profile of SSF could enable data processors to send an out-of-band consent on/off signal to data processors and for them to pass it along to other third parties.

It's long been known that – just like in the railroad world – interoperability standards have an outsized role in making digital identity successful. It seems embracing interop for user-centric permissions is not just a noble pursuit – it's a necessity.

## New Belief 3: Data Shielding Requires Potent Solutions

For personal data to flow safely and usefully for all parties, it requires shielding – which in turn requires potent solutions. They need to be so potent that they pave new business models while ripping up old ones.

The belief that **data shielding requires potent solutions** should embolden us to make lasting change. To get into the right frame of mind, it's worth reviewing solutions we thought would have an effect – but haven't.

You might think **Apple's App Tracking Transparency** feature counts as potent. Its launch in April 2021 made cross-app tracking more difficult and – along with Google's ongoing "cookiepocalypse" threat – had a seismic effect on Facebook's business model.

"The potential loss of \$10 billion in ad sales revenue accounts for nearly 8% of Facebook's yearly revenue – and the market reacted, with the stock price dipping 26%."

– [Forbes](#) in 2022



But tech loopholes quickly began to appear, and in a few short years Meta has more than recovered from its stock stumble.



You might expect **GDPR** to be potent enough to help us turn the corner. Unfortunately, after six years of enforcement and billions in infrastructure investments and fines, data monetization continues to be powerfully lucrative; the cavalry is not coming.

ETid	Country	Date of Decision	Fine [€]	Controller/Processor
ETid-2479	ROMANIA	2024-11-04	1,000	Blackcab Systems SRL
ETid-2478	ROMANIA	2024-10-30	15,000	Untold SRL
ETid-2472	ROMANIA	2024-10-28	5,000	Vodafone Romania S.A.
ETid-2469	IRELAND	2024-10-24	310,000,000	Linkedin
ETid-2471	ROMANIA	2024-10-23	10,000	Profi Rom Food SRL
ETid-2473	SPAIN	2024-10-22	180,000	IBERCAJA BANCO, S.A.
ETid-2482	NORWAY	2024-10-21	20,800	Grue municipality
ETid-2470	ROMANIA	2024-10-16	3,000	Your Consulting SRL
ETid-2461	IRELAND	2024-09-27	91,000,000	Meta Platforms Ireland Limited
ETid-2463	ITALY	2024-09-26	4,000	CI & DI Food s.r.l.

Showing 1 to 10 of 2,483 entries

Ten most recent GDPR fines as of publication time, out of 2,483 entries.

Image credit: [GDPR Enforcement Tracker](#)

Famed privacy activist [Max Schrems](#), speaking at the [EIC](#) conference, shared a study of more than 1000 data protection officers. 74% said that a Data Protection Authority walking into the door of an average data controller would “surely find relevant GDPR violations.” And national authorities are struggling too; over 300 of the GDPR complaints lodged by his company [noyb](#) have been pending for more than two years.

“Right now we see, after the first hype of GDPR, more of a downward spiral.”

– Max Schrems at EIC24

**After six years of enforcement and billions in fines,  
the cavalry is not coming.**



You might be hopeful for the potency of **selective disclosure** techniques, particularly cryptographically protected ones like Zero Knowledge Proofs (ZKPs). But as we've seen, they're no panacea. What's the latest news on this front?

Leading cryptographers submitted some tough feedback on the EU's Architecture Reference Framework (ARF) for digital identity wallets, demanding use of anonymous credentials. However, there's evidence it won't help.

Timothy Ruff, one of the inventors of AnonCreds, acknowledges that correlation and re-identification of individuals is trivially easy. And a recent Gartner Hype Cycle for Privacy placed consent management, ZKPs, and decentralized identity in the "trough of disillusionment." ZKPs were judged to be "obsolete before plateau."



What solutions might be potent enough?

## Potent Solution? Privacy-Enhancing Technologies – DISAPPOINTING

**Privacy-enhancing technologies (PETs)** have been a favored area of privacy innovation and research for many years. Wikipedia divides them into “soft” and “hard” technologies, ones where a trusted third party has a role or doesn’t, respectively.

It’s good for individuals’ wishes to be made enforceable by tech; I have even contributed innovations on the “soft” side. Unfortunately, even Wikipedia’s compendium of “hard” solutions doesn’t inspire confidence, so it can’t be relied on excessively.



That’s on the one hand. On the other, **privacy isn’t secrecy**, as the User-Managed Access (UMA) community has long observed. You can’t lock yourself away in a metal box and emit no data. Absolute secrecy isn’t viable because sharing data is necessary – and desirable – for too many reasons. We have to share something, and so we have to strive for better options.

On the gripping hand, interacting with any online service **exposes something**, which in turn can be used to correlate you against your will. Even the Signal service can’t prevent it.

## Potent Solution? Fully Homomorphic Encryption – PROMISING

Green shoots of progress are appearing around an interesting technology: **fully homomorphic encryption (FHE)**. Here's a nice [explainer video](#). Put simply, FHE allows data to be processed while remaining in encrypted form. You can run computations on encrypted data and get results that are encrypted to you.

In my EIC conference address, I advocated for a second look at FHE based on the new wave of AI-supporting chips that are bringing FHE compute into a reasonable range. Since then, Apple [open-sourced](#) its FHE solution and is now delivering real-life applications. It's also being used in some privacy-preserving Web3 technologies.

**We may start seeing new solutions built on FHE that move the needle.** It's possible to imagine new companies competing with old ones by offering to remove the classic privacy tradeoff in operating on personal data.

Some cautions are in order. The aforementioned UMA community, in addition to believing privacy isn't secrecy, also observes that **privacy isn't encryption**. Not only can encryption be broken or bypassed; it's also simply a technique that needs a solution environment. Beware of just "doing crypto" and thinking it solves human challenges. [Enveil's CEO put it well](#).

"Homomorphic encryption libraries provide the basic cryptographic components for enabling the capabilities, but it takes a lot of work including software engineering, innovative algorithms, and enterprise integration features to get to a usable, commercial grade product."

– Ellison Anne Williams in [The Stack](#)

We'll also have to learn how to optimize data schemas and queries to enable real-world performance. Nonetheless, I'm hopeful that with the right innovation, FHE could count as potent enough.

**FHE could remove the classic privacy tradeoff in operating on personal data.**



## Potent Solution? Unfollow Everything 2.0 – PROMISING

As already noted, **GDPR hasn't been potent enough** to produce improved outcomes. But sometimes key legal frameworks or decisions can unlock potent new solutions.

**Unfollow Everything** was a neat technical trick invented by UK-based Louis Barclay in 2021. He created a popular browser extension that allowed Facebook users to **automatically unfollow** all their friends, groups, and pages, clearing out their News Feed while keeping their connections. Researchers even started testing it in measuring happiness. It gave users vastly more control – but then Facebook banned Barclay for life and legally forced him to take down the tool.



Fast forward to May 2024. A lawsuit was filed on behalf of Ethan Zuckerman, a professor at UMass Amherst, because he wants to create **Unfollow Everything 2.0**. Under implicit threat from the prior action, he wants legal cover before creating his tool. Meta has asked to toss the suit but says it won't countersue yet. The Electronic Frontier Foundation (EFF) has filed an amicus brief supporting Zuckerman's immunity.

Having to depend on single court cases to enable you to make major digital-life decisions is unfortunate – and it can take a long time. But there's no doubt such cases can have impact. I'm hopeful a win here could unlock newly viable market options for user-permissioned data sharing.



## Personal Data Innovation Scenarios

By combining solution ideas and applying some creativity, we can imagine some innovative ways forward that could boost personal data control.

### Scenario 1: Selective Disclosure With Public Awareness

We've seen that **selective disclosure** looks surprisingly weak as a privacy preservation and user choice technique. In the face of easy re-identification attacks, is it pointless, or still valuable?

People still want their sharing preferences respected and enforced, and it's better to **minimize disclosure** than maximize it.

However, as Sam Smith has emphasized in his [research](#), it's easy for individuals to be misled by the selective disclosure experience and erroneously believe no additional data was captured. This suggests a need for better public awareness.

**I believe:** We should press ahead on enabling selective disclosure, while educating people about what is done with the data they shed.

**I predict:** People will get wise to the reality of selective disclosure, just like they did with passwords ("make them secure") and 2FA ("better to turn it on") over the last decade. They already know cookies and similar tech are tracking them.

### Scenario 2: Chain-Link Confidentiality With Enforcement

Many privacy analyses end up recommending a **chain-link confidentiality** approach, often out of exasperation when a PET doesn't do the trick. The idea, first [proposed](#) in 2012, is to impose clear legal constraints that "stick" to each step of downstream use and sharing.

Is such an approach enough?

Using today's consent system, if we could prove consent was given using **Consent Receipts**, and could look up precise legal rights for a data operation using the **Consent Name Service**, we'd be ahead of the game. If downstream data processors were required to subscribe using the **Shared Signals Framework** to a feed of consent withdrawals, it could help ensure that consent is consistently respected across different systems.

In a post-consent future, if we had ready-made sets of universal **machine-readable privacy terms** of the sort I hope will emerge from the [IEEE P7012 group](#), we could use them in **right-to-use personal data licenses** of the sort discussed in my [paper](#) with Lisa LeVasseur. They would have robust **chain-link** properties. Applying a **digital rights management** (DRM) approach on top by leveraging **FHE** could lead to better enforcement.

**I believe:** Legal and operational controls are necessary, but still amount to relatively weak promises.

**I predict:** FHE and similar cryptographic protections will be the pièce de résistance in giving individuals greater control over data use.

### Scenario 3: Open Banking's Regulatory Approach

Explicit "privacy regulation" has produced little improvement. By contrast, financial services institutions in many jurisdictions – no strangers to heavy regulation – have been subject to **Open Banking guidelines and mandates** focused on security, customer choice, and fintech innovation, with arguably much greater success in security and privacy outcomes. UK Open Banking, PSD2, and the aforementioned FDX demonstrate the power of combining interoperable security requirements with consent UX guidelines.

**I believe:** The history of privacy laws as "things that happen to data subjects" is a disempowering legacy that's too difficult to overcome; achieving user-driven permissions requires a modern regulatory approach.

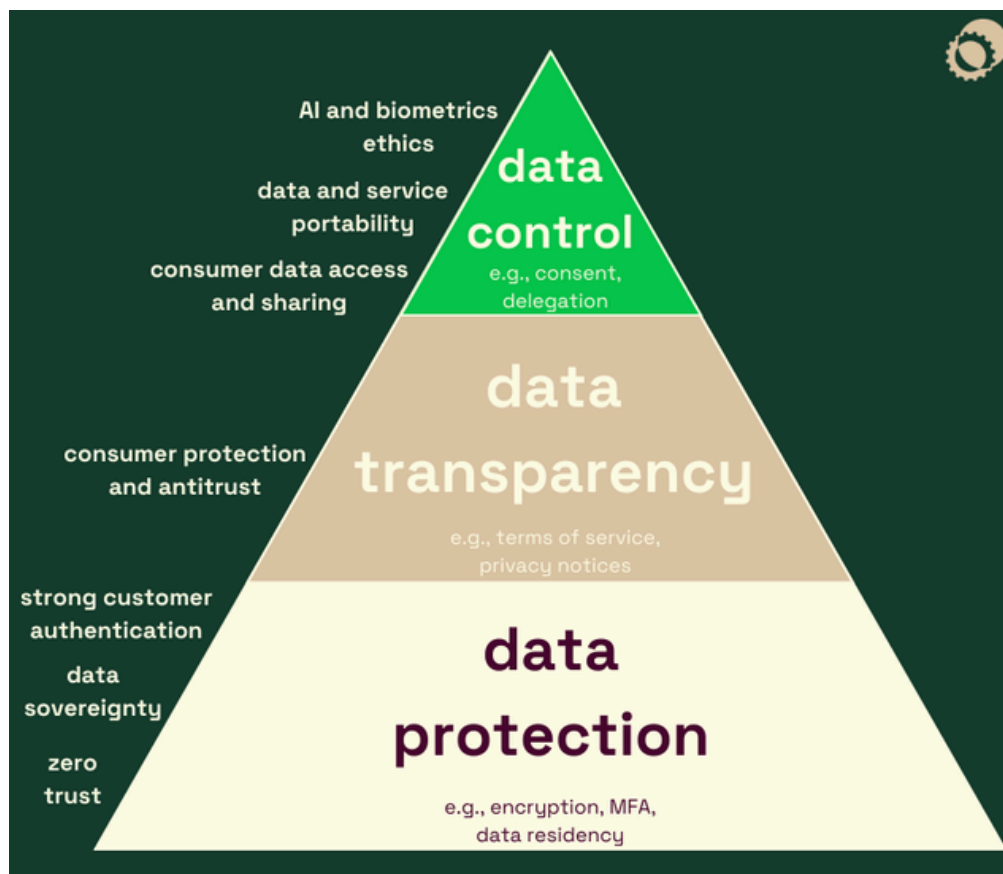
**I predict:** Open Banking's "open API" approach will inspire future laws.

## Next Steps for Identity Pros

Living up to our beliefs isn't without its challenges.

The point of anchoring on new beliefs is not to ensure airtight secrecy with zero data sharing; it's to enable healthy online relationships between individuals and businesses. Consent and privacy issues are increasingly symptoms of a larger ethical and regulatory landscape.

What can you do, given the extraordinary power and “stickiness” of data monetization and the platforms that underlie this business model?



Those who practice the IAM discipline have a key role in serving as “vital and vibrant counterparts to privacy and information security,” as the IDPro organization’s vision for the industry puts it.

Take these steps to improve your company’s relationship with individuals and their personal data.

## Step 1. Find Personal Data Allies Hiding Within Your Organization

The **consumer-facing IAM** (CIAM) function often carries a burden of satisfying organization-wide security and privacy goals that it's not prepared to bear. As one example, you can't offer a "right to be forgotten" option in good faith if you don't know where all of the user's data is.

The average enterprise ecosystem for leveraging personal data involves **data not fully visible in IAM systems** and contributes to a company's bottom line directly, unlike the typical IAM implementation.

Get closer to your marketing and data colleagues and the tech used in your organization's **personal data value chain** writ large. The exercise can open your eyes to additional data and user trust risks in play and let you apply your IAM expertise in solving key business problems like improving customer conversions, upsell, and loyalty.

Common customer data platform (CDP) challenges include obtaining a unified view of a customer across data sources, coordinating customer treatment across channels, and delivering customer profiles to systems that need it. You can become part of the solution while ensuring better **data protection, transparency, and control**.

Reveal these stakeholders by following a "day in the life" of representative data fields, such as home address and mobile device type:

**Plot** the stages of data handling for each field, including collection, verification, storage, usage in different applications, and third-party sharing, along with any consent gathered and revoked.



**Track** the owner of the relevant infrastructure and process at each stage.



**Capture** the value of the data as reported by each stakeholder.

## Step 2. Leverage Your Company's Personal Data Innovation Appetite

With internal relationships improved, you're prepared to answer tough questions about how far new privacy, consent, and end-user control initiatives could go in your organization. Privacy is rarely a business differentiator today, although sufficiently potent solutions applied as part of an innovation strategy can change that equation. Is your organization...

**Firmly wedded to the existing data monetization regime?**

This is a fact of life in many enterprises. Plan on **tactical moves** to start. Integrate a comprehensive CIAM approach to unify interfaces for managing permissions, while identifying data value chain risks.

**Concerned about the security and trust costs of personal data?**

The door to innovation has opened a bit; the banking sector is alert to these risks. Partner with payments owners to consider solutions that promote **transparency** and trustworthiness at a minimum.

**Confident about customer value gains from user control features?**

You face a great innovation opportunity! Apps that integrate with platforms such as Apple Health often allow **fine-grained data sharing controls**. Partner with product owners to amplify such capabilities.

**Hanging its hat on personal autonomy as a corporate mission?**

You are in rare circumstances. Offer help in implementing dramatic **data shielding** solutions while bringing awareness to the privacy- and autonomy-destroying risks in current approaches.

**Privacy is rarely a business differentiator today.  
Sufficiently potent solutions can change  
that equation.**





### Step 3. Test the Execution of Your Innovation Plans

Don't just ensure new projects adhere to compliance mandates, which aren't improving the situation. And don't just commit to qualitative principles (such as FIPPS) without identifying the **quantitative outcomes** you seek. Decide what you believe, and then test to see if you're living up to those beliefs.

If you like the new beliefs proposed above, try using the following as principles and sample metrics, keeping in mind that your own metrics will depend on your initiatives.

#### Let Individuals Determine Their Relationship Status

- Do web pages avoid placing tracking cookies (or similar) on a user's device before offering cookies and getting agreement?
- Can users change their mind about previously shared data and be offered proof that the change has been implemented?

#### Make Permissions About Digital Assets Interoperable

- Are all consent withdrawals communicated to third parties who previously received the data?
- Do services respect Do Not Track signals?

#### Use Potent Data Shielding Solutions

- Do de-identification methods come with provable results?
- Are encryption methods quantum-resilient at a minimum?

# Privacy Is Context, Control, Choice, and Respect

I believe, and I hope you do too.

If, as UMA aficionados have observed, privacy isn't secrecy and it isn't encryption, and if it isn't even compliance, what is it? UManitarians say **Privacy is context, control, choice, and respect.**

Even though digital consent has missed the mark in its current incarnations, I believe identity pros can push the edge of the envelope, shaping a future where the **human capacity to make an informed, uncoerced decision** is respected while businesses simultaneously benefit from relationships with humans.

Here's to shifting from coercion to true cohesion, from chaos to compatibility, from chance to control – and a promise kept.



## DEVELOP IRRESISTIBLE IDENTITY STRATEGIES



### ADVISORY

**Make Your Vision Actionable**  
Advisory, board, and fractional  
Chief Technology Officer /  
Chief Strategy Officer services



### COACHING

**Standards Coaching**  
Insights on understanding  
and impacting the identity  
standards landscape



### SPEAKING

**Workshops and Speaking**  
Education, perspective, and  
foresight delivered engagingly  
by an industry pioneer



### CONSULTING

**Technology Consulting**  
Governance and oversight of  
IAM tech implementation and  
integration projects

Venn Factory believes in making the future of identity actionable. We drive identity, security, and privacy success by helping the tech world develop irresistible product and go-to-market identity strategies that are poised to have immediate operational impact.