MICKAI™

MICKAI EBOOK SERIES · No. 21

The Rights of the Record.

Provenance as a civic right in the age of automated decisions.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

19 June 2026 · v1 · mickai.co.uk

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO register, named inventor Mickarle Wagstaff-Irons · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

FOREWORD

A note from the author

I have spent the last several years building a system that decides things, and the longer I have done it, the more convinced I have become that the most important question is not how well a machine decides but whether the person on the receiving end can reach the record of that decision. My name is Micky Irons. I am the founder of Mickai and the named inventor on its patent portfolio, which is owned by Mickai LTD. I write this book not as a technologist explaining a product, but as a citizen who has watched the architecture of everyday life quietly migrate into systems that no one outside the building can see. We are being decided about, constantly, and most of us cannot ask the machine to show its working.

This book exists because I believe provenance is a civic right and not a technical luxury. When a benefits claim is refused, when a loan is declined, when a border is closed to you, when a child is flagged by a risk model, something happened inside a system. A chain of inputs produced an output that changed your life. The ordinary citizen is told the outcome and almost never given the record. I think that is the wrong way round. I think the record should be the first thing you are owed, reachable by you, verifiable by you, and not erasable by the institution that produced it.

I want to be careful and honest about what I am claiming. Mickai is a Sovereign Intelligence Operating System, not a finished utopia. Some of what I describe here is built and running, some is designed and filed and not yet in production, and I will mark the difference plainly throughout. I have no interest in selling you a future that does not exist. The argument of this book does not depend on my system being perfect. It depends only on a principle: that automated power without a reachable record is power without accountability, and a society that accepts that has given something away it will struggle to win back.

So this is a short book with a single spine. It moves from the problem, the disappearing record, to the mechanism, what a sealed and verifiable record actually requires, to the evidence and the economics of building one, and finally to what citizens, institutions, and engineers should now do. I have written it in plain language because the people most affected by automated decisions are rarely the people invited into the technical conversation. They should be. The rights of the record belong to all of us, and the first step in claiming them is understanding what we have been quietly losing.

Micky Irons

Founder and named inventor, Mickai LTD · 19 June 2026

THE VANISHING RECORD

When machines decide and the record disappears, the citizen is left holding an outcome with no way to reach its cause.

The decision you cannot see

Consider an ordinary morning that does not feel like a confrontation with power. You apply for something online. You wait. A message arrives telling you the answer is no. There is a reference number, a polite paragraph, perhaps a phone line that loops you back to the same paragraph. What there is not, almost anywhere, is the record: the specific inputs that were read, the model that read them, the weighting that turned a person into a score, and the moment the score became a refusal. The outcome is delivered with total confidence and zero traceability. This is now the texture of modern administration, and we have grown used to it without ever agreeing to it.

The strange thing about automated decisions is that they generate enormous quantities of internal evidence and then keep almost none of it. A human decision-maker leaves notes, a paper trail, a memory you can subpoena. A machine pipeline produces logs, feature vectors, model versions, and intermediate states, far more detailed than anything a human clerk ever recorded. The information exists at the instant of the decision. The citizen simply cannot reach it, and most of it is overwritten or aged out within days. We have not lost the record because records became impossible. We have lost the record because no one was required to make it reachable, and the default of every system is to discard what it is not obliged to keep.

What makes this acute is the asymmetry. The institution holds the model, the data, the logs, and the legal team. You hold a reference number. When you challenge the decision, you are asked to disprove a conclusion whose reasoning you have never been shown. You are arguing against a verdict with the evidence locked in the other side's building. In any courtroom this would be recognised instantly as a denial of due process. In the administrative state and the private platform, it has become the normal operating condition, and familiarity has dulled our sense that anything is wrong.

> **We have not lost the record because records became impossible, we have lost it because no one was ever required to make it reachable.**

I do not think the people building these systems are villains. Most of them are solving a narrow problem under deadline, and the question of whether the affected citizen can later reach the record is simply not on the specification. That is precisely the issue. Accountability that depends on the goodwill of

busy engineers is not accountability. It is luck. The vanishing record is not a conspiracy, it is an emergent property of building decision systems without treating the record as a first-class output. And what emerges by default tends to favour whoever holds the machine.

The cost of this is not only individual injustice, though there is plenty of that. It is the slow erosion of the idea that power should be answerable. Every decision that cannot be inspected teaches the citizen that inspection is not for them. Over time a society learns to stop asking. That learned silence is more dangerous than any single bad decision, because it dismantles the expectation that produced good government in the first place. The record is not a technical detail. It is the thread that ties power to consent, and we have been letting it fray.

Why an outcome is not an explanation

Institutions often respond to this concern by offering more communication. You will be told the reason for the decision in plain language. A loan was declined due to your credit history. A claim was rejected because the criteria were not met. This feels like an explanation, and it is meant to. But a reason written after the fact, by a communications layer that did not itself make the decision, is not a record of how the decision was made. It is a story about the decision, composed to be acceptable. The two can diverge completely, and the citizen has no way to tell whether they have.

The gap between an output and its provenance is where most injustice now lives. A model can produce the right answer for the wrong reason, or the wrong answer for a reason that would be plainly illegal if anyone could see it. Bias does not announce itself in the summary paragraph. It hides in the weighting, in the training data, in a proxy variable such as a postcode that quietly stands in for something the law forbids you to use directly. An after-the-fact explanation, however sincere, cannot expose any of this, because it is generated downstream of the decision and has no privileged access to what actually happened inside it.

There is a deeper problem with treating the explanation as a substitute for the record. An explanation is a claim. A record is evidence. When an institution tells you why it decided, you are being asked to trust an assertion. When an institution shows you a verifiable record of what it actually computed, you are being given something you can check against an independent standard. The first depends entirely on the honesty and competence of the institution. The second does not. A right that depends on the goodwill of the party you are challenging is not a right at all.

> **An explanation is a claim, a record is evidence, and only one of them survives a determined dispute.**

This distinction matters most in exactly the cases where it is hardest to insist on. The powerful institution facing a credible challenge has every incentive to offer the smoothest possible explanation and to never produce the underlying record. If the only thing the citizen is owed is an explanation, the institution controls the entire evidentiary frame. It writes the reason, it grades the reason, and it decides when the reason is sufficient. The asymmetry of the vanishing record is not solved by better explanations. It is solved only by making the record itself something the citizen can demand and verify.

I want to be clear that explanations have their place. A human being denied something deserves words they can understand, not a wall of feature vectors. The point is not to replace explanation with raw data. The point is that the explanation must be anchored to a record that exists, that the citizen can reach, and that an independent party can check. Explanation without an underlying record is theatre. Record without explanation is inaccessible. The right of the record is the insistence that we are owed both, and that the words must be answerable to the evidence beneath them.

The Mickai pantheon.

The law that almost says it

We are not starting from nothing. Several bodies of law already gesture toward the right I am describing, even if none of them quite completes it. European data protection law contains a much-discussed provision about decisions based solely on automated processing, and a debated idea that individuals are owed meaningful information about the logic involved. Administrative law has long held that public bodies must give reasons. The instinct that power should be answerable to the person it affects is old and well established. What is new is that the machinery of decision has outrun the machinery of accountability.

The trouble is that these protections were written for a world of human files and discrete decisions. Meaningful information about the logic involved is a beautiful phrase that collapses the moment you ask what it concretely requires from a system processing millions of cases through a model no single person fully understands. Reason-giving duties assume a reason exists somewhere a person could write down. When the decision is distributed across a pipeline, a model version, and a dataset, the law's good instincts arrive at a technical reality they were not designed to grip.

More recent regulation has begun to close the gap. Rules emerging around high-risk automated systems, including the European Union's AI Act, increasingly demand logging, traceability, and record-keeping as conditions of deployment. This is genuine progress, and it moves the conversation

from explanation toward provenance, which is the right direction. But there is a recurring weakness. The records these rules require are typically held by the operator, in the operator's systems, under the operator's control. The citizen is still not the one who holds the key. The fox has been asked to keep a detailed diary of the henhouse.

> **The law has the right instinct and the wrong custody, it asks the operator to keep the record the citizen most needs to reach.**

This is the crux of the civic argument. A record that the deciding institution can edit, withhold, or quietly lose is not a guarantee. It is a courtesy that can be revoked at the worst possible moment. For the right of the record to mean anything, the record must have properties the institution cannot unilaterally override. It must be sealed so it cannot be altered after the fact. It must be timestamped against something external. And ideally it must be reachable by the citizen without the institution's permission. The law is reaching toward these properties. It has not yet named them clearly enough to require them.

So the task ahead is partly legal and partly technical, and the two have to be developed together. The law can declare a right, but a right with no enforceable technical substrate is a promise on paper. The technology can build a sealed record, but a sealed record with no legal standing is a clever artefact no court will look at. The rest of this book is about both halves: what a record must technically be in order to deserve the citizen's trust, and what we must collectively demand so that the law treats such a record as the citizen's due. The instinct is already in our law. We have to give it teeth.

WHAT A TRUSTWORTHY RECORD REQUIRES

A record only earns trust when it is sealed, timestamped, and reachable without the deciding party's permission.

Sealing the moment a decision is made

If we accept that the citizen is owed a record, the next question is brutally practical. What must that record actually be in order to be worth anything in a dispute? A log file in a database does not qualify, because the party that owns the database can change it. A screenshot does not qualify, because it proves nothing about what the system actually computed. The record we need has to be sealed at the moment the decision is made, in a way that makes later alteration detectable. This is not a comfort feature. It is the difference between evidence and an assertion.

In the system I build, every consequential action is sealed into what we call an Open Audit Record, an OAR. The principle is simple even if the cryptography is not. At the moment a decision is taken, the relevant state is captured and signed, so that any later change to that record breaks the seal and is immediately visible. The signature uses a post-quantum standard, ML-DSA-65 under FIPS 204, which is a published NIST standard and not something I invented. I want to be precise about that, because the credibility of a record depends on its standing on recognised cryptography rather than a private scheme only its author trusts.

The choice of a post-quantum signature is deliberate and not a marketing flourish. Records about decisions can matter for decades. A benefits determination, a medical triage, a custody assessment can be litigated or revisited long after it was made. A signature scheme that is secure today but breakable by tomorrow's computing is not adequate for evidence meant to last. Anchoring the seal to a standard designed to withstand quantum attack is simply taking seriously the idea that the record must outlive the moment. We are not protecting a transaction. We are protecting a citizen's ability to challenge a decision years from now.

> **A record that the institution can quietly edit is not evidence, it is an opinion wearing the costume of proof.**

Sealing also changes the incentives inside the institution, which is half the point. When every consequential action is written into a sealed record at the moment it happens, the option of quietly losing an inconvenient decision disappears. The record is not something assembled later, when a dispute arises and the lawyers are involved. It exists from the instant the decision is made, and it cannot be tidied. This is uncomfortable for institutions accustomed to controlling the narrative, and that discomfort is the feature, not the bug. Accountability that can be edited is not accountability.

I should be careful here about the line between built and designed. The sealing of records into OARs under the post-quantum standard is core to how the system works today. Other capabilities that surround custody of the keys, such as automated key rotation and trustee succession, are designed and filed as part of the architecture and are not all in production yet. I draw this line deliberately, because a book arguing for verifiable records would be self-defeating if it overstated its own. The seal is the foundation. The custody machinery around it is being built outward from that foundation, and I will not pretend the whole edifice is finished.

The Mickai pantheon.

Anchoring provenance to something the institution cannot move

A sealed record solves one problem and exposes another. If I sign a record, I have proved that the record has not changed since I signed it. I have not proved when I signed it, or that I did not simply create the whole thing this morning and backdate it. For a record about a decision to carry weight, its existence at a particular time must be anchored to something outside the control of whoever made it. Otherwise the institution can manufacture a clean history after the fact, and a forged record signed honestly is still a forgery.

This is why provenance in the system anchors to Pantheon, a sovereign Layer 1 that is itself anchored to Bitcoin. The structure is a base chain together with fifteen application chains, with a fixed-supply token called PAN. The detail of the token economics matters less to the civic argument than the architectural fact: by anchoring records to a chain that is in turn anchored to a large, independent, widely-witnessed ledger, the existence of a record at a point in time becomes something no single institution can rewrite. The anchor is external by design, because an internal anchor is no anchor at all.

I am aware that mentioning a blockchain in a book about civic rights invites a particular weariness. The field has earned its scepticism. So let me be plain about what the anchor is for and what it is not. It is not a currency story and it is not a speculative instrument in this context. It is a clock and a witness. Its only job in the architecture of the record is to make the timing and existence of a sealed decision independently checkable, so that a citizen disputing a decision can point to evidence that the institution cannot have fabricated after the dispute began.

> **Provenance is only as strong as its anchor, and an anchor the institution can move is decoration, not proof.**

The combination is what matters. A sealed record proves integrity, that the content has not changed. An external anchor proves existence and timing, that the record was there before the argument started. Together they give a citizen something genuinely powerful: a decision they can prove was made at a certain time, in a certain form, and has not been altered since. That is a far stronger position than a reference number and a polite paragraph. It moves the citizen from begging for an explanation to holding evidence, and that shift in posture is the entire point of the exercise.

None of this requires the citizen to understand cryptography, any more than using a bank requires understanding a vault. The properties have to hold underneath, verifiable by independent experts and open tools, so that ordinary people can rely on them without becoming specialists. That is how trust in infrastructure has always worked. We do not each test the bridge before we cross it. We rely on the fact that it was built to a standard others can and do check. The record deserves the same treatment: built to a published standard, anchored to an independent witness, and trustworthy precisely because its trustworthiness does not depend on trusting the institution that produced it.

Sovereignty means the record runs on your own ground

There is one more property a trustworthy record requires, and it is the one most often missing from well-intentioned transparency schemes. The record must live somewhere the deciding party does not solely control. If your evidence sits entirely inside the institution's cloud, on the institution's terms, it can be throttled, delayed, or made conditional on your good behaviour. Custody is destiny. Whoever holds the record ultimately controls whether the right to it is real, and a right held at someone else's discretion is a privilege by another name.

This is why the system is built as a Sovereign Intelligence Operating System rather than a service you log into. Mickai is not an app. It is an operating environment in which fifty specialised brains, twenty-five domain and twenty-five operational, run on the operator's own hardware and are capable of working offline. The significance for the civic argument is that the intelligence and the records do not have to depend on a remote provider's permission. The decision and its provenance can live on ground the operator actually holds, rather than in a facility that can change its terms or disappear overnight.

Sovereignty cuts in more than one direction, and honesty requires acknowledging it. For an institution, running the system on its own hardware means it cannot blame a vendor for the records, the records

are its own and it must answer for them. For an individual, the same property means data sovereignty in the literal sense: the record about you can be held by you, on hardware you control, rather than living only in a system that decided against you. The same architecture that makes institutions more accountable makes individuals more powerful. That symmetry is intentional, and it is why I keep insisting that sovereignty is a civic question and not merely a technical one.

> **Custody is destiny, and a right to a record held only in the other side's building is a right held at their pleasure.**

Building for sovereignty imposes real discipline on what the system can be. It is why the models are specialised to run on hardware the operator owns rather than assuming an endless connection to a distant data centre. We are actively training our own models now, fine-tuning and specialising open foundations such as Llama 3.2 and Qwen 2.5 and building a sealed corpus, with the funded roadmap scaling toward fully native weights over time. I describe this honestly as a trajectory that is already under way rather than a finished state. The principle, though, is fixed from the start: the system must be able to stand on its own ground, because a record that depends on someone else's infrastructure inherits that infrastructure's power over you.

I do not claim this resolves every tension. Sovereignty can be misused, and a record held by a determined wrongdoer on their own hardware is harder for legitimate authority to reach. These are real trade-offs and I will not wave them away. But the failure mode we have today, where records about citizens live entirely inside the institutions that produced them, is not neutral ground. It is already a choice, and it is a choice that favours power over the individual. Sovereign custody is not a perfect answer. It is a deliberate rebalancing toward the person who has, until now, held only a reference number.

The Mickai pantheon.

THE EVIDENCE AND THE ECONOMICS

The case for verifiable records is not only moral, it is practical, lawful, and ultimately cheaper than the alternative.

What it costs to keep nothing

Institutions resist the idea of comprehensive, sealed records by reaching first for the cost argument. Keeping everything, sealing everything, anchoring everything, surely this is expensive and slow. It is a fair question and it deserves a real answer rather than a slogan. But the honest accounting has to include the cost of the current arrangement, which is rarely counted because it is paid in places that do not show up on the system's own budget. The cost of keeping nothing is enormous. It is simply borne by other people.

Consider what happens now when a decision is challenged. Lawyers reconstruct, badly, what a system might have done. Experts are hired to argue over logs that were never designed to be evidence. Cases drag for years because no one can produce a clean record of what was actually computed and when. Appeals multiply because the absence of a verifiable record means every dispute starts from zero. The administrative cost of opacity is staggering, but it is spread across courts, ombudsmen, regulators, and the unpaid time of the people fighting their own cases. None of it appears on the line item of the institution that chose not to keep the record.

There is also the cost of error that is never caught. A system that keeps no reachable record is a system that cannot easily learn it was wrong. Mistakes that would be obvious in a clear audit trail instead accumulate silently, sometimes for years, until a scandal forces an inquiry that costs more than a decade of record-keeping would have. The pattern is depressingly familiar, and the Post Office Horizon scandal is the textbook case. A body automates a decision, errors compound invisibly, the harm eventually surfaces, and the inquiry discovers that the records needed to understand what happened were never properly kept. The opacity that looked cheap was the most expensive option available.

> **Opacity is not free, it is the most expensive option we have, and the bill arrives later in someone else's name.**

Set against this, the cost of sealing records is modest and falling. Cryptographic signing is fast and cheap, measured in milliseconds and fractions of a penny per record. Anchoring to an external ledger costs a fraction of a single disputed case. Storage is among the cheapest resources we have. The economics that once made comprehensive record-keeping genuinely burdensome belong to an earlier era of computing, and they no longer hold. What persists is not a cost problem but an incentive

problem. The institution that would pay to keep the record is not the one that would pay the price of its absence, and until that gap is closed, opacity will keep looking cheap to the only people who get to choose.

This is why I think the economic argument ultimately favours the record, once you count honestly. A society that builds verifiable records into its automated decisions pays a small, predictable, upfront cost and avoids a large, chaotic, recurring one. It trades the expensive theatre of reconstruction for the cheap discipline of keeping. The institutions that resist are not protecting the public purse. They are protecting their own narrow budget line at the expense of the wider system, and a serious policy maker should be able to see straight through that accounting.

Provenance as infrastructure, not feature

The reason verifiable records are not yet standard is partly historical and partly architectural. Most decision systems were built with the record as an afterthought, a logging module bolted on near the end, configured to keep as little as compliance demanded. Treating provenance as a feature guarantees it will be the first thing cut under deadline and the last thing anyone can rely on. A right cannot rest on a feature that the next sprint might quietly remove. It has to rest on infrastructure that the system cannot function without.

The alternative is to make the record structural, so that producing a sealed, anchored record is not an optional add-on but the very mechanism by which a decision is enacted. In the architecture I have described, a consequential action is not complete until it is sealed into an Open Audit Record. The record is not a report about the decision written afterward. It is the form the decision takes. You cannot have the action without the record, because the sealing is part of how the action happens. That inseparability is what turns a good intention into a reliable property.

This is the difference between a system that can produce an audit trail if asked and a system whose normal operation is an audit trail. The first depends on someone configuring it correctly and leaving it configured. The second cannot be quietly switched off without breaking the thing it is meant to do. For a civic right, only the second is acceptable. We should not have to trust that the logging was turned on. The record should be a load-bearing wall, not a decorative panel that can be removed when it becomes inconvenient to whoever holds the building.

> **Make the record the way the decision is enacted, not a note written about it afterward, and it can no longer be quietly switched off.**

Building this way is harder, and I will not pretend otherwise. It constrains how the system is designed from the first line. It rules out architectures that would be simpler and faster if you did not care about provenance. The discipline shows up everywhere, in how state is captured, in how keys are managed, in how the whole thing is structured so the record cannot be separated from the act. Much of the patent portfolio behind the system, one hundred and one filed UK patent applications with around two thousand two hundred and thirty four claims owned by Mickai LTD, exists precisely because doing this

properly required solving problems that simpler systems get to ignore.

I mention the filings not to wave a number but to make a point about seriousness. Treating provenance as infrastructure is not a slogan you can adopt by changing your marketing. It is a different way of building that touches every layer, and it generates genuinely hard technical problems that have to be solved and, where novel, protected. These are filed applications, under examination at the UK Intellectual Property Office. The honest claim is that we have done the work to make the record structural rather than decorative, and that the work was substantial enough to be worth protecting. The number is evidence of effort, not a trophy.

The Mickai pantheon.

The individual as a sovereign party

Most of the transparency conversation imagines the individual as a complainant, someone who shows up after a bad decision to ask for an explanation. I want to propose a more ambitious frame. The individual should be a sovereign party to decisions made about them, holding their own copy of the record, on their own terms, from the moment the decision is made. This is data sovereignty in its fullest sense, not the right to ask for your data, but the right to hold the record of what was done to you as a matter of course.

This reframes the whole relationship. Today the citizen is structurally downstream, dependent on the institution to surface, explain, and eventually release whatever record exists. As a sovereign party, the citizen holds a verifiable record from the outset, sealed and anchored, that no one can alter or withhold. The dispute, if it comes, starts from a position of evidential parity rather than supplication. That is a profound change in the balance of power, and it is achievable with technology that already exists, not technology we have to wait for.

The economics of this favour the individual in a way that is unusual and worth dwelling on. Normally, increasing an individual's power against an institution requires lawyers, time, and money, resources distributed exactly opposite to need. A verifiable record inverts that. The cost of holding a sealed record is the same whether you are wealthy or poor, and once held it does the work that would otherwise require expensive reconstruction. Provenance, built as infrastructure, is one of the rare interventions that gives the most leverage to the people who can least afford the alternative.

The citizen should not arrive at a dispute as a supplicant but as a party who already holds the evidence.

I am conscious that holding a record is not the same as understanding it, and that a sealed file means little to someone without the tools to read it. This is a real gap and it is where the sovereign operating environment earns its place. The same fifty brains that can run on the operator's own hardware can help an individual make sense of the records they hold, turning a sealed artefact into something a person can actually interrogate in plain language. The capability to read your own record has to come with the right to hold it, or the right is hollow. A vault you cannot open is just a heavier kind of lock.

I will mark the line once more, because it matters. The architecture for individuals to hold and read their own sealed records is core to how the system is designed. Some of the surrounding custody machinery, the dead-man's switch, the trustee succession that decides what happens to your records if you cannot act, the long-term key management, is designed and filed and not uniformly in production yet. I describe the destination clearly while refusing to dress the journey up as already complete. The principle is fixed and the direction is set. The honest statement is that we are building toward the citizen as a sovereign party, and we are not yet all the way there.

CLAIMING THE RIGHT

Turning provenance into a lived civic right will take citizens, institutions, and engineers each doing their distinct part.

What citizens should demand

Rights are not granted by the systems they constrain. They are demanded, and then defended. If provenance is to become a civic right rather than a technical curiosity, the demand has to start with the people most affected by automated decisions, which is to say nearly everyone. The first thing to demand is simple and concrete: when a machine makes a consequential decision about you, you are owed a record of that decision that you can hold, that you can verify, and that the institution cannot quietly alter. Not an explanation generated afterward. A record, sealed at the moment of decision.

The second demand is about custody, and it is the one institutions will resist most. The record must not live only inside the system that produced it. A right to a record you cannot reach without the institution's cooperation is not a right, it is a hope. Citizens should demand that records about them are reachable independently, anchored to something external, held in a form that does not depend on the goodwill of the party they may one day need to challenge. This is the harder ask, and it is the one that actually changes the balance of power rather than merely softening its appearance.

The third demand is for honesty about what systems can and cannot do. Citizens should be deeply sceptical of any institution that offers transparency as a feeling rather than a property. A reassuring paragraph is not a record. A dashboard you can look at but not export is not custody. A promise of fairness with no verifiable trail is a request for trust dressed as a guarantee. The questions to ask are blunt. Can I hold this record. Can I verify it. Can you alter it without my knowing. If the answers are no, no, and yes, you are being offered theatre, and you should name it as such.

> **A right to a record you cannot reach without the institution's cooperation is not a right, it is a hope.**

These demands are not radical. They are the digital extension of principles we already hold about due process and the answerability of power. We do not think it strange that a court keeps a record, that a contract is written down, that a person accused is shown the evidence against them. The strangeness is that we have allowed automated decisions to escape these basic expectations simply because they are new and complicated. The demand for the rights of the record is a demand that old principles apply to new machinery. There is nothing exotic in insisting that power leave a trace the citizen can reach.

And citizens should make the demand collectively, because individually it is too easy to dismiss. One person asking for their record is a nuisance to be managed. A population that expects records as a matter of course is a political fact that systems must be built around. The history of rights is the history of demands that became too widely held to refuse. Provenance can follow the same path, but only if enough people understand that the record is theirs to claim and stop accepting the reference number as the end of the conversation.

The Mickai pantheon.

What institutions should build

Institutions, public and private, will eventually have to provide verifiable records, whether by conviction or by regulation. The ones that move early will find the transition far easier than the ones that wait to be forced. So I want to speak directly to the people who build and run decision systems, because much of what needs to change is in their hands and a good deal of it is more achievable than they assume. The first move is to stop treating the record as a compliance afterthought and start treating it as a core output of the system, as important as the decision itself.

Concretely, this means sealing decisions at the moment they are made, using recognised cryptographic standards rather than private schemes. It means anchoring records to something external so their timing and existence can be independently verified. It means designing for the citizen to hold a copy, not merely to request one through a process the institution controls. None of these are exotic. They use published standards and available infrastructure. What they require is the decision to make provenance structural, and the willingness to accept the accountability that comes with records you cannot quietly edit.

I understand the fear underneath the resistance. A verifiable record means an institution can be held to what it actually did, with no room to reconstruct a more flattering account later. For an institution that has been getting things wrong, that is genuinely threatening. But for an institution that is getting things

right, it is the strongest possible defence. A sealed record is as good at vindicating a sound decision as it is at exposing a bad one. The institutions that fear the record most are telling on themselves, and the ones acting in good faith should want it more than anyone.

> **A sealed record defends the institution that decides fairly as powerfully as it exposes the one that does not.**

There is also a competitive logic that the early movers will feel first. As citizens come to expect verifiable records, the institutions that already provide them will hold a real advantage in trust, and trust is becoming the scarcest resource in any system that decides about people. The bank, the agency, the platform that can say here is your sealed record, verify it yourself, will earn a credibility that no marketing can buy. Provenance is not only a duty to be discharged. It is, for the institution willing to embrace it, an asset, and the ones who see that early will not have to be dragged.

I will say plainly that this is the bet behind everything I build. I am betting that the future belongs to systems that can prove what they did, not merely assert it. The Sovereign Intelligence Operating System exists to make that proof structural, so that an institution running it produces verifiable records as a matter of normal operation rather than special effort. I am not asking institutions to take my system on faith. I am asking them to accept the principle, build toward it however they choose, and recognise that the era of decisions without reachable records is ending whether they prepare for it or not.

What we owe the record, and each other

I have argued that provenance is a civic right, that a trustworthy record must be sealed and anchored and reachable, that the economics favour keeping over discarding, and that citizens, institutions, and engineers each have a part to play. I want to close by stepping back from the mechanism to the meaning, because the technical case only matters in the service of a human one. The reason any of this is worth the effort is not elegant cryptography. It is the dignity of the person on the receiving end of a decision they did not make and cannot see.

A society reveals what it thinks of its members by what it lets them see of the decisions that shape their lives. A society that decides about people in the dark, and hands them only outcomes, has decided that those people are objects of administration rather than parties to it. A society that gives people a reachable record of the decisions made about them has decided that they are owed an account, that power must answer, that the citizen is not merely managed but respected. The rights of the record are, in the end, a statement about whether we treat each other as people or as cases.

I am not naive about how hard this will be. The institutions that benefit from opacity are powerful, the technical work is genuinely demanding, and the legal frameworks are still catching up to machinery that has already outrun them. I have spent years on a single corner of this problem and I am acutely aware of how much remains undone, in my own work and in the wider effort. But difficulty is not an argument against a right. It is a description of the work the right requires, and the work is worth doing precisely because the alternative is a future we should not accept.

A society reveals what it thinks of its members by what it lets them see of the decisions that shape their lives.

I have tried throughout this book to be honest about the line between what is built and what is designed, between what runs today and what we are working toward. The seal on the record, the anchoring of provenance, the sovereign operating environment running on the operator's own hardware, these are real and running. The fuller custody architecture, the long-term key management and succession, is designed and filed and not all in production. We are training our own models now and scaling toward fully native weights as the work is funded. I tell you this because a book demanding verifiable records would be a poor thing if it played fast and loose with its own claims. The right of the record begins with telling the truth about the record.

So this is my close, and it is less a conclusion than a handing over. The rights of the record are not mine to grant and not any institution's to withhold. They belong to all of us, and they will exist only to the degree that we collectively insist on them. I have built what I can build and argued what I can argue. The rest is a civic act, the slow, stubborn, shared work of deciding that when a machine decides, the person decided about is owed a record they can reach. We are owed it. I think we should claim it. And I think the time to begin is now, while the architecture of the automated age is still being poured and there is still a chance to set the record into its foundations.

The Mickai pantheon.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder and chief executive of Mickai LTD (Companies House 17166618, registered office 20 Wenlock Road, London, N1 7GU) and named inventor on the Mickai SIOS patent corpus: 101 filed UK patent applications, around 2,234 claims. Trade mark Mickai registered at UK00004373277.

Profiles

mickai.co.uk

crunchbase.com/person/micky-irons

linkedin.com/in/mickyirons

References and further reading

· Pasquale, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015.

· O'Neil, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, 2016.

· Eubanks, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St Martin's Press, 2018.

· National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA). U.S. Department of Commerce, 2024.

· Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

· Wachter, Sandra, Mittelstadt, Brent, and Floridi, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 2017.

· Citron, Danielle Keats. Technological Due Process. Washington University Law Review, 2008.

· Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.