Before There

Was a Password

A short Introduction About The Philosophy and Politics of Secrecy

BSidesVienna · 27 June 2026 · Workshop with Iryna

Agenda

0	Opening & Hook	*5 min*
1	Impulse I — The Anthropology of Secrecy	*8 min*
✎	Exercise I — What would you never say?	*7 min*
2	Impulse II — From the Cave to the GDPR	*8 min*
✎	Exercise II — A World Without Secret	*10 min*
3	Impulse III — Why We Should Think This Through	*5 min*
◉	Landing & Open Discussion	*2 min*

Opening

How many of you have a password manager?

Opening

How many of you have ever had a secret?

Why did we start keeping secrets in the first place?

IMPULSE I – *8 minutes*

The Anthropology of Secrecy

https://www.france-voyage.com/visuals/photos/lascaux-ii-42071_w1000.webp

Secrecy is about relationships — not information

"The secret is not about hiding a content. The secret is about the social relation it produces."

—Michael Taussig
Defacement, 1999

~ 150

Dunbar's Number

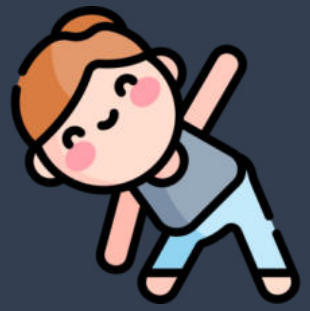
Social group size at which humans can track who knows what, who trusts whom.

17.000 BCE

Lascaux Cave

Deep inside, not at the entrance. Already a social infrastructure of selective access.

Before there was encryption, there was …



EXERCISE I
– *7 minutes*

What would you never say?

Turn to the person next to you. 90 seconds each.

Think of something you know that you would never post publicly — not because it's dangerous, not because it's illegal, but just because it feels wrong.

Why does it feel wrong?

You don't have to share the secret. Just the reason for keeping it.

- It's private
- It's nobody's business
- It would be misunderstood
- It could be used against you

We keep secrets because of a social models, relationships etc.

[The extraction of behaviorial data is so powerful (...) because it reads your social hesitations – the things, you almost searched for, the messages you started and deleted].

— Shoshana Zuboff, 2019
The Age of Surveillance Capitalism

IMPULSE II – *8 minutes*

From the Cave to the GDPR

The architecture of secrecy is never neutral

17,000 BCE

Lascaux

Selective access as social infrastructure

The Roman state

Wax seal, “mystery”

Initiation of in- and out-groups

1948

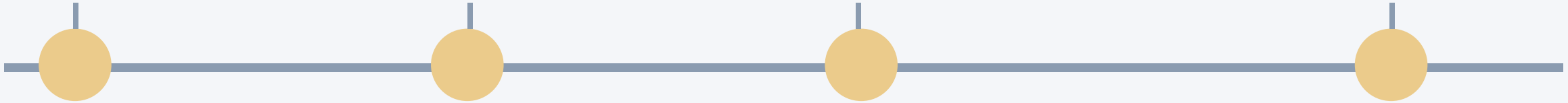
UDHR Art. 12

Privacy enshrined as a human right — for the first time, globally

2018

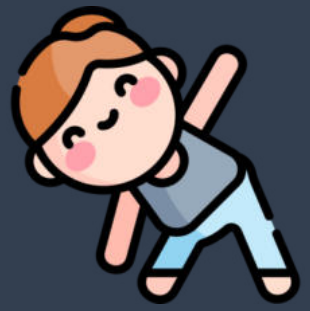
GDPR

Right to be forgotten. Right to portability. Information as self-ownership.



The architecture of secrecy is never neutral.
It always serves someone.

The question is: who?



EXERCISE II
– *10 minutes*

Radical Transparency

Groups of 4–5. Each group picks one scenario.

Answer: (1) What breaks immediately? (2) What might work better?

Scenario A

All government communications are public by default — in real time.

Scenario B

All corporate financials, including individual salaries, are publicly accessible.

Scenario C

All medical records are public, but fully anonymized.

Scenario D

All code in public infrastructure is open source by legal mandate.

Scenario E

All communications metadata (who contacted whom, when, how often) is visible.

Key points

Power asymmetry

Trust as precondition

The Panopticon problem

The practical paradox

Privacy ≠ Secrecy

"The difference between privacy and secrecy is this:

one is used to protect,

the other is used to hide."

— Renee Slansky, The Dating Directory

IMPULSE III – *5 minutes*

Why We Should Think This Through

“The map is not the territory”
— Alfred Korzybski

Contextual Integrity

Information flows inappropriately not because it is private or public — but because it violates the norms of the context in which it was shared.

— Helen Nissenbaum, 2004

Medical info

Shared with your doctor → flows appropriately to your specialist, not your employer.

Zero Trust

Don't assume the perimeter. Verify every request in context. A contextual question.

Threat Modeling

Who is the adversary? What do they want? Always a contextual question.

The philosophy came first.

The technology followed.

It always does.

Who drew the line between what this system knows and what it doesn’t?

And whose interests does that line serve?

That’s not a rhetorical question.
It’s a design question.

TAKE AWAY

What happened when the line between what we show and what we hide doesn’t just blur – it disappears entirely?

https://lumiere-a.akamaihd.net/v1/images/image_7049663a.jpeg?region=0%2C0%2C800%2C1200

Before There Was a Password

—

The Philosophy and Politics of Secrecy

Workshop | BSidesVienna 0x7EA | June 27, 2026
Track: Ethical and philosophical implications of hacking / History & Philosophy of computing

---

References

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Dunbar, R. I. M. (1992). Neocortex size as a constraint on group size in primates. *Journal of Human Evolution*, *22*(6), 469–493. https://doi.org/10.1016/0047-2484(92)90081-J

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, *L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books. (Original work published 1975)

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. Copernicus Books.

Taussig, M. (1999). *Defacement: Public secrecy and the labor of the negative*. Stanford University Press.

United Nations. (1948). *Universal declaration of human rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Workshop Overview

Inhalt

1. Opening Hook

How many of you have a password manager?"

And how many of you have ever had a secret — not a password, not a PIN — just something you knew that you decided, consciously, not to tell anyone?
Same mechanism. Completely different history.

We spend enormous energy protecting information. Firewalls, encryption, access controls, zero-trust architectures. But almost nobody in this field ever asks the question that sits underneath all of it: *Why did we start keeping secrets in the first place?*
Not 'how do we protect data?' — we're good at that. But *why does the category 'secret' even exist?* Who invented it? And — what would we lose, and what might we gain, if we got rid of it?
That's what this workshop ist about.

---

2. Impuls I — The Anthropology of Secrecy

A cave painting. Lascaux, roughly 17,000 BCE is not just art. This is, arguably, one of the earliest acts of selective disclosure in human history.
The cave at Lascaux was not at the entrance. It was deep inside. You had to know it was there. You had to be brought there. That is already a social infrastructure of secrecy — someone knows, someone doesn't, and that difference is *meaningful*.

The anthropologist Michael Taussig, in his 1999 monograph *Defacement: Public Secrecy and the Labor of the Negative*, published by Stanford University Press, argues that the secret is not about hiding a content. The secret is about the social relation it produces. The moment you say 'I have a secret,' you've created an asymmetry. A power dynamic. An inside and an outside (Taussig, 1999, p. 5).
That's the first thing I want you to hold onto: **secrecy is not fundamentally about information. It's about relationships.**

Now: why would early humans need that asymmetry? Robin Dunbar's landmark 1992 study, published in the *Journal of Human Evolution*, showed that neocortex size across 36 primate genera correlates directly with social group size — and that for humans, this cognitive ceiling sits at roughly 150 stable relationships. That is not a cultural artifact. That is neurobiology. Dunbar argued that the human brain evolved precisely to track who knows what, who trusts whom, who owes what to whom (Dunbar, 1992, pp. 469–470). Secrets are a tool for social navigation. They signal membership, they create alliance, they mark the boundary between in-group and out-group.
In other words: before there was encryption, there was the campfire. And not everyone was allowed to sit at it.

---

3. Übung I — What would you never say?

Setup (1 min): Turn to the person next to you. You have exactly 90 seconds each. One of you answers this question:
'Think of something you know that you would never post publicly — not because it's dangerous, not because it's illegal, but just because it feels wrong. Why does it feel wrong?'
Then switch. The other person answers. You don't have to share the content of the secret. Just the *reason* for keeping it.

Discussion (4 min): Collect reasons from the room. Write them visibly on a white-board or flipchart.
Cluster examples:
"It's private" → What does 'private' actually mean as a category?
"It would be misunderstood" → By whom? Why is interpretation asymmetrical?
"It's nobody's business" → What makes something 'your business' and not someone else's?
"It could be used against me" → Power. Always power.
Debrief (2 min): Notice what just happened. None of you kept a secret because of a technical threat model. You kept it because of a *social* one. Because of what it does to relationships, to perception, to power.

Shoshana Zuboff, in her 2019 book *The Age of Surveillance Capitalism*, describes this with precision: the extraction of behavioral data is so powerful not because it reads your passwords, but because it reads your social hesitations — the things you *almost* searched for, the messages you *started* and deleted (Zuboff, 2019, pp. 8–11). The technical and the social are not separate threat surfaces. They are the same surface.

---

4. Impuls II — From the Cave to the GDPR

Secrecy scales. That's the story of the last three thousand years. The Roman state classified military dispatches. Medieval guilds guarded trade knowledge as corporate secrets — the term 'mystery' in 'mystery guild' comes from the Latin *ministerium*, meaning a craft or trade, but it also bled into the sense of hidden knowledge. The guild didn't just train you. It initiated you. It drew a line between those who knew and those who didn't.
Jump to 1948. The Universal Declaration of Human Rights, Article 12: *'No one shall be subjected to arbitrary interference with his privacy.'* For the first time in history, a global document enshrines the *right to have a secret sphere* as a human right — not a privilege, not a courtesy, a right (United Nations, 1948).
And then — 1995. The EU Data Protection Directive. The first serious legal attempt to say: your information, even when held by someone else, is still *yours*. The GDPR in 2016 — in force from 2018 — tightened that further. The right to be forgotten. The right to data portability. These are not technical specifications. They are philosophical positions about what it means to own information about yourself (European Parliament & Council of the European Union, 2016).
But here's the tension: every single system we've built to protect secrecy — encryption, access control, classification levels — also *enables* secrecy. And secrecy, in the hands of power, looks very different than secrecy in the hands of a private individual.
WikiLeaks. The Panama Papers. NSA's PRISM program. Corporate NDAs. State secrets. National security exemptions in GDPR. The philosopher and security technologist Bruce Schneier put it plainly in his 2003 book *Beyond Fear*: security is fundamentally about trust — and the asymmetry of who controls information determines who holds power (Schneier, 2003). The architecture of secrecy is never neutral. It always serves *someone*. The question is: who?

---

5. Exercise II — Radical Transparency

Setup (2 min): Split into groups of four or five. Each group gets one of the following scenarios. You have five minutes to answer two questions:
What breaks immediately?
What, surprisingly, might work better?
Scenario A: All government communications — emails, internal memos, meeting minutes — are public by default, in real time.
Scenario B: All corporate financial information — including individual salaries — is publicly accessible.

Scenario C: All medical records are public, but fully anonymized.
Scenario D: All source code deployed in public infrastructure is open source by legal mandate.
Scenario E: All communications metadata — not content, but who contacted whom, when, and how often — is publicly visible.

Discussion (5 min): Collect the result "breaks immediately" and "might work better" from each group.
Key themes to surface:
Power asymmetry: radical transparency harms the weak before it constrains the powerful. Why? George Akerlof's Nobel Prize-winning 1970 paper on information asymmetry in markets — *The Market for Lemons* — showed that when one party to a transaction knows more than the other, the less-informed party bears the greater risk. Applied to radical transparency: the powerful have lawyers, PR departments, and spin infrastructure. The powerless have none of that. Transparency without equal interpretive capacity is not fairness — it's exposure (Akerlof, 1970, pp. 489–492).
The Panopticon problem: Bentham's prison, Foucault's analysis — if everyone is watched, everyone *performs*. Authenticity collapses. Foucault argued in *Discipline and Punish* that the genius of the panopticon is not observation but *the internalization of the observer* — people discipline themselves when they believe they might be seen (Foucault, 1977, pp. 201–203). Every transparent system risks producing exactly this effect at scale.
Trust as precondition: Bruce Schneier's observation that security is about trust, not just secrecy. Can trust exist without the *possibility* of a secret? Schneier (2003) argues that trust requires vulnerability — the option to *not* disclose is the condition under which genuine disclosure becomes meaningful.
The practical paradox: end-to-end encryption exists because we want to communicate *selectively*. Selective disclosure is not a bug in the information ecosystem — it is the ecosystem. Nissenbaum's (2004) contextual integrity framework explains why: every social context has its own appropriate information flows, and the category "public" is always context-dependent.
Debrief (3 min): None of these scenarios work cleanly. Some fail catastrophically. Some reveal something interesting about why our current defaults are the way they are. But the exercise isn't about finding the right answer. It's about noticing that 'secret' and 'public' are *choices* — not laws of nature. And that the line between them has always been drawn by someone with the power to draw it.

Before we go into the last impulse, I want to leave one sentence in the room. It's not from an academic paper. It's from a relationship coach — and it's sharper than most research I've read on the topic.

“The difference between privacy and secrecy is this: one is used to protect, the other is used to hide." Rene Slansky

That distinction is exactly what we've been circling around for the last 35 minutes. Secrecy hides. Privacy protects. Every system we build either does one or the other — or quietly does both, depending on who's holding the keys.

---

6. Impuls III — Why should we think this through?

Quote — "The map is not the territory." — Alfred Korzybski
Now let us to spend the last few minutes on the thought experiment itself.

Why should we imagine a world without the categories 'secret' and 'public'? Not because it's achievable. Not because it's desirable in simple terms. But because the exercise *reveals the architecture*.
Helen Nissenbaum, the philosopher and privacy theorist, introduced the concept of *contextual integrity* in her landmark 2004 article in the *Washington Law Review*. Her argument: information doesn't flow inappropriately because it's private or public — it flows inappropriately when it violates the norms of the *context* in which it was shared. Medical information shared with your doctor flows appropriately to your specialist, but not to your employer. Not because it's 'secret' in some absolute sense — but because the context has norms (Nissenbaum, 2004, pp. 136–138).
That's a much more useful frame than secret/public. And we only find it when we start questioning the binary.
In information security, we do this all the time — we just don't call it philosophy. Threat modeling asks: *who is the adversary, and what do they want?* That is a contextual question. Zero Trust architecture says: *don't assume the perimeter holds — verify every request in context.* That is a contextual question. And Michel Foucault, in *Discipline and Punish* (1977), showed us the flipside: that surveillance — the *removal* of secrecy from those without power — is itself a technology of control. When the warden can see every cell, the prisoner doesn't need to be watched to behave. The *possibility* of being seen is enough (Foucault, 1977, pp. 195–200). That logic runs through every access log, every audit trail, every CCTV system we've ever built.
The philosophy came first. The technology followed. It always does.

---

7. Landing — And the last one

We build systems to protect secrets. We build laws to protect privacy. We build cultures around what can and cannot be said, known, disclosed. All of that is important work. And none of it is neutral. The next time you design an access control policy — or argue for end-to-end encryption — or configure a firewall rule — ask yourself: *who drew the line between what this system knows and what it doesn't? And whose interests does that line serve?* That's not a rhetorical question. It's a design question.

Thank you.

Before we back to our daily business — a piece of homework for the week after. There's a film called *Hide and Seek*. The title alone is the thesis of this workshop. Watch it. It asks what happens when the line between what we show and what we hide doesn't just blur — it disappears entirely.
Have fun with the film!
See you very soon!