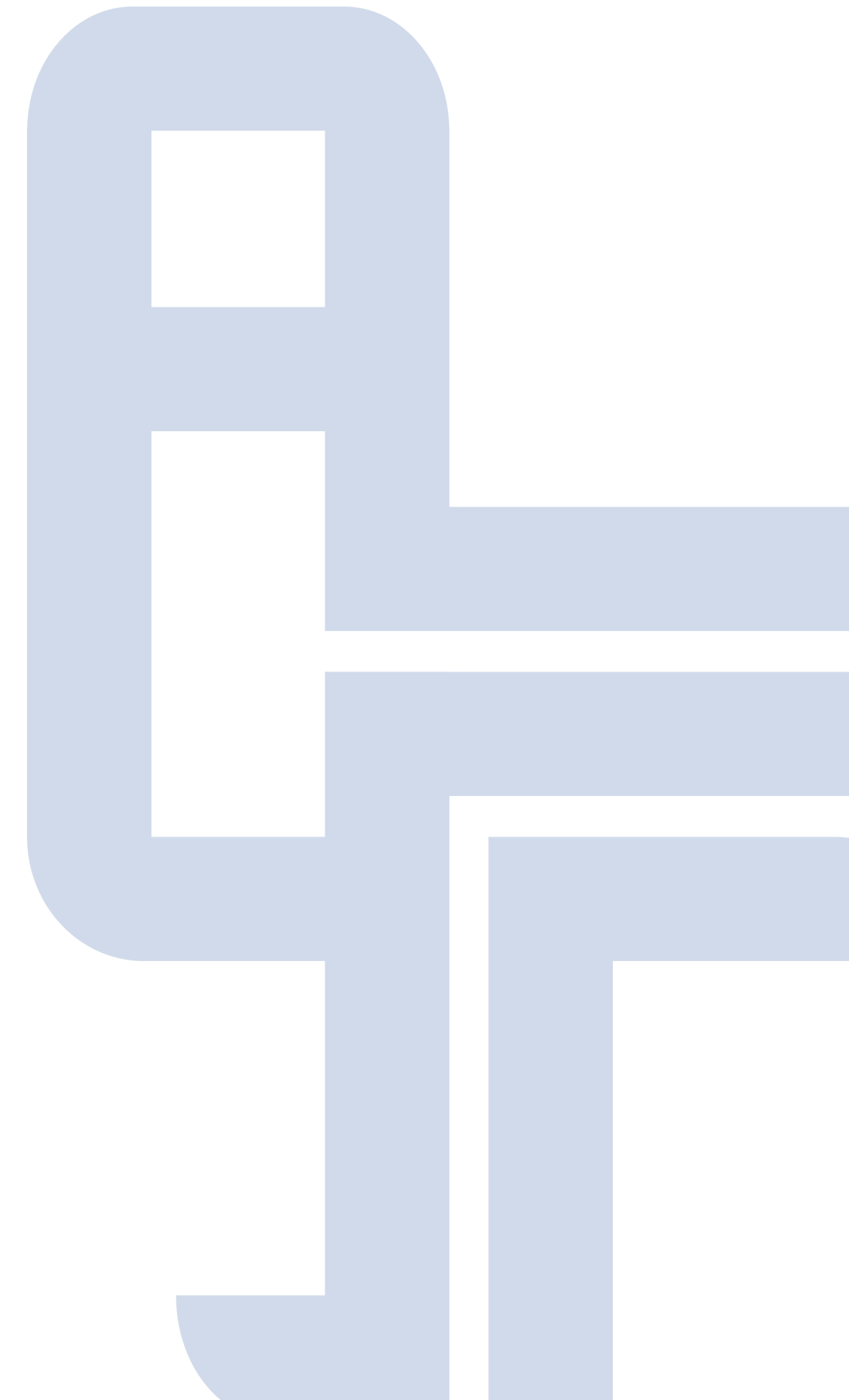




The Peace Coalition

Presentation to the World Bank

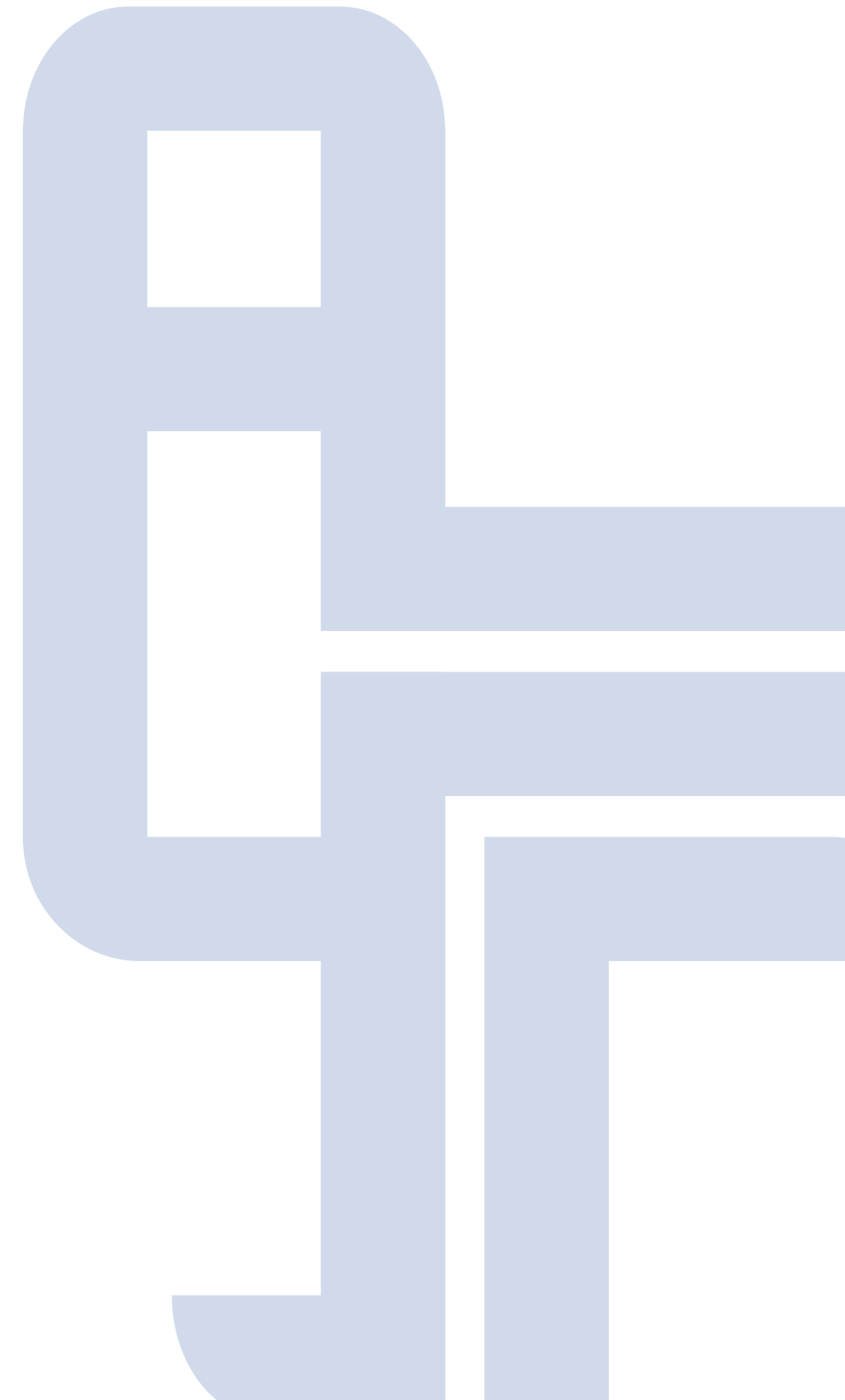
May 10, 2023





Michael Cholod

Secure & Anonymous Mobile Claims Registry



From Rwanda to Bosnia, Sudan to Kosovo, Liberia to Sri Lanka, the critical importance of ensuring the realisation of refugees' and internally displaced persons' right to housing and property restitution has become increasingly recognised.

[OHCHR - March 2007](#)

10 percent of Africa's rural land is registered. The remaining 90 percent is undocumented and informally administered, which makes it susceptible to land grabbing, expropriation without fair compensation, and corruption. Again, these consequences fall hardest on women farmers who are often the only breadwinners in their families.

[The World Bank - July 2013](#)

82.4 million people have been forced to flee their homes due to wars and global weather crisis.

[UNHCR - February 2022](#)

2 billion people—over a quarter of the world's population—lack a fundamental human right: the right to property.

[New America - February 2022](#)

6.5 million refugees have fled Ukraine since the start of hostilities by Russia.

[UNHCR - February 2022](#)

The Problem

Housing, land, and property rights form the basis of any society. The ownership of property has historically been a tool for wealth building and the control of power and additional resources.

Insecure land rights also keep communities from mitigating and adapting to the impacts of climate change. These issues often stem, in part, from a lack of [verifiable and secure ownership documents](#), inaccurate maps, and the inability of government agencies to record and defend property rights.

The Opportunity

Worldwide, billions of people cannot access the most basic benefits of property rights due to a lack of ownership documents, inaccurate maps, and ineffective government agencies to defend tenure security. Modern technology can greatly simplify the recording and defending of property rights at scale, yet these tools are not being properly utilized.

Tech innovators often misunderstand the policies, politics, and societies that their solutions must operate within, while government officials are often unaware or skeptical of available tools

X7%49Kn

Property
Damage Claim
submitted



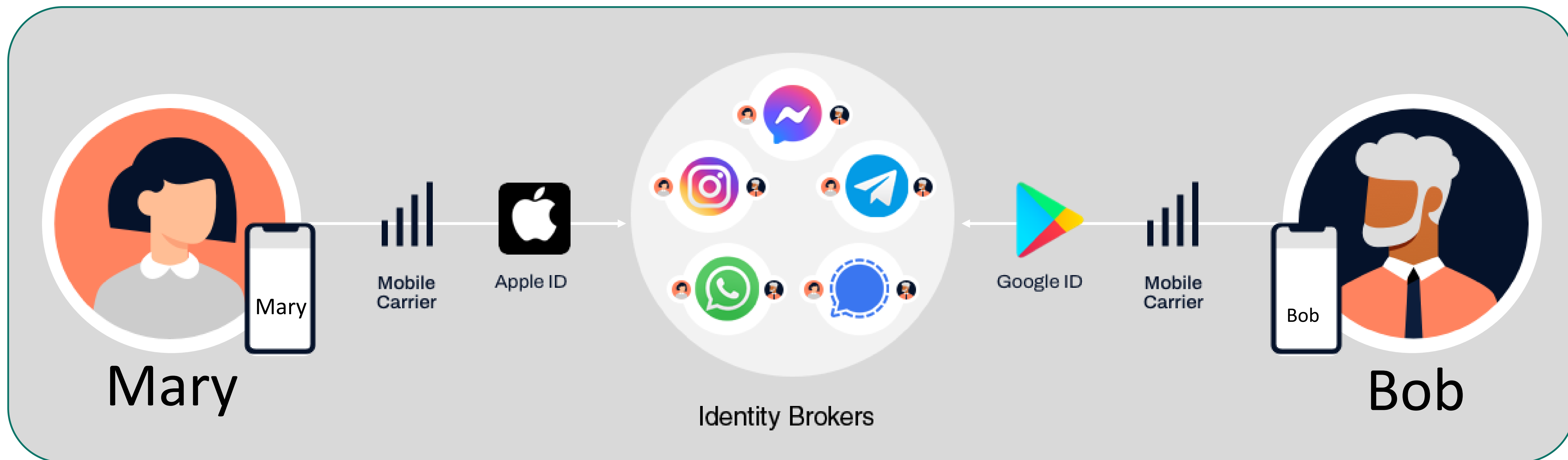
NEW
AMERICA

“In an ideal way yes, [if you are a refugee], you would like your making of a claim to an authority to be private. But what we're seeing is that you don't get that because it's not in place yet. If there was a trusted digital platform that a refugee could engage to say, okay, I'm going to make my claim, I'm going to upload my evidence, including who I am, where I am, what exactly my evidence is and all these other people that will attest to me - we need that!”

So, if you're unsure about having your data being divulged to one's enemies, then just keep it on your phone for now, but do gather it, do interview grandma before she passes away so she can give you the whole history of occupation of your land, and it could be corroborated - **just keep it on your phone.**”

The Problem of Connecting online

People are forced to rely on third party web services as identity brokers for our connections and to store our personal data.



Third party web services are easily controlled or disabled

This graphic shows Internet connections in Russia. The **red** and **blue** nodes represent internal connections between Russian citizens. The **green** Tier 1 access nodes represent connections to the Internet outside Russia. Internet access to any public website can be controlled by operators of the **red** or **blue** nodes, who can explicitly block lookups of its DNS name, access to its IP address or network, or both.

- Access to the Internet outside Russia could be completely disabled by disconnecting the Tier 1 **green** nodes.
- All metadata and public posts by Russian users of **red** and **blue** nodes are effectively in the hands of the Russian government and susceptible to identification and intimidation.
- VPNs are often used to circumvent access restrictions imposed by Russian authorities, but VPNs are centralized and easily victim to network surveillance, subscriber requests, or bribery as they aggregate many users with similar anti-censorship objectives.
- Ironically, using a VPN increases a users attack surface, creating a high-value target that explicitly collects information about the activities of its users.

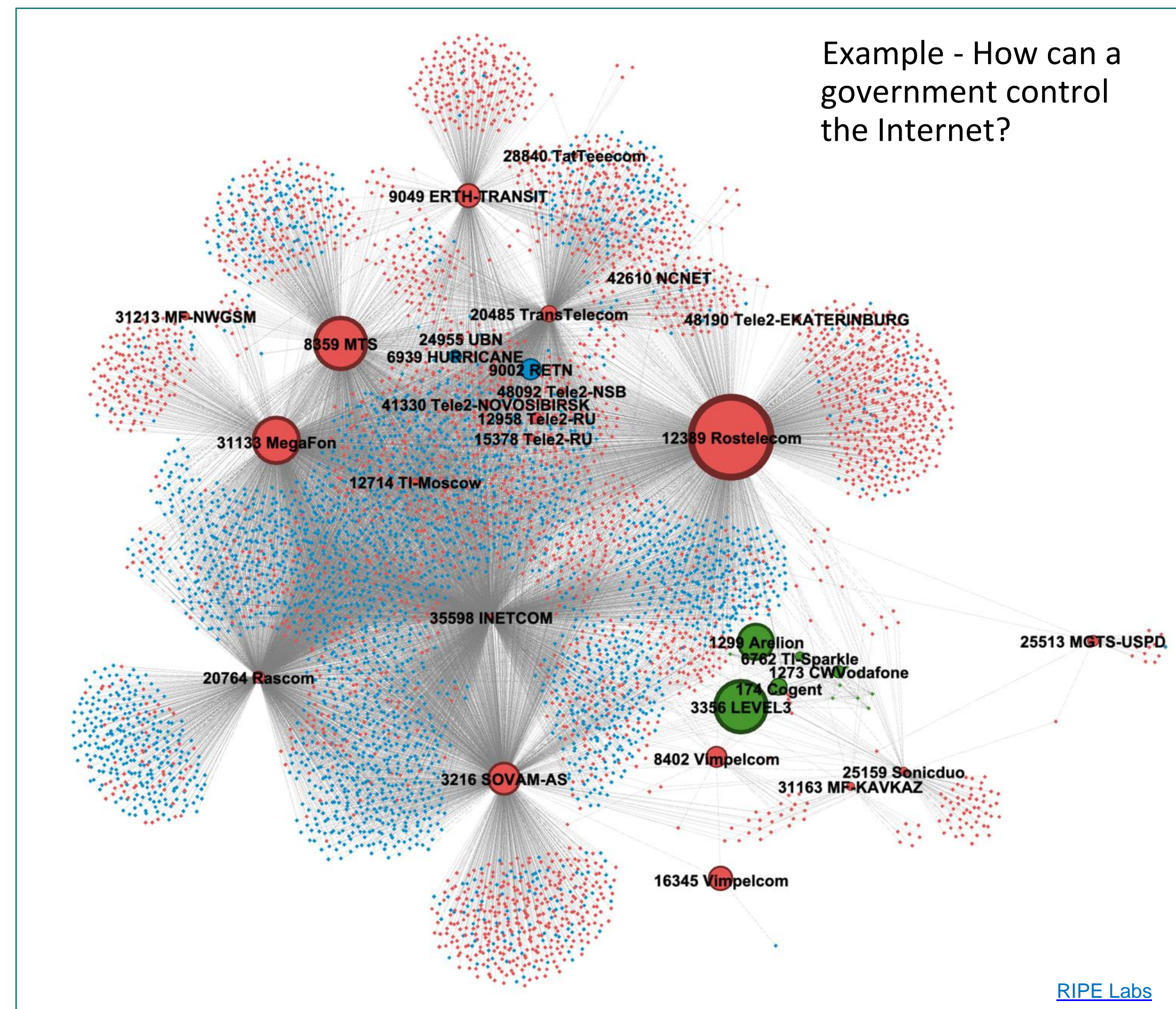
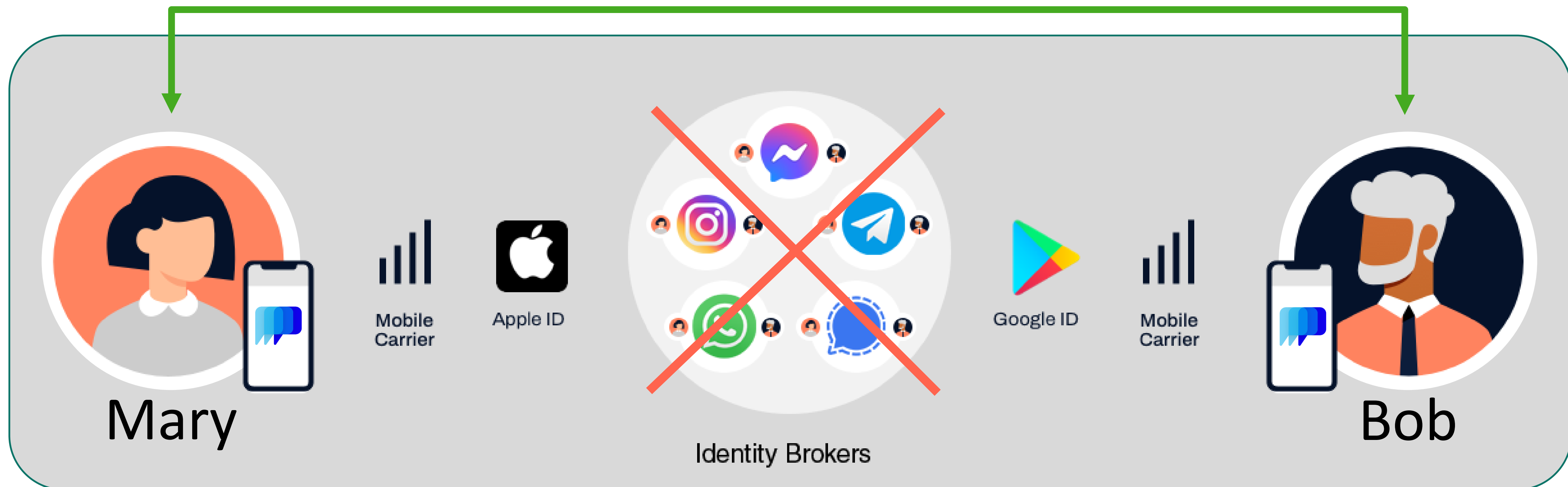


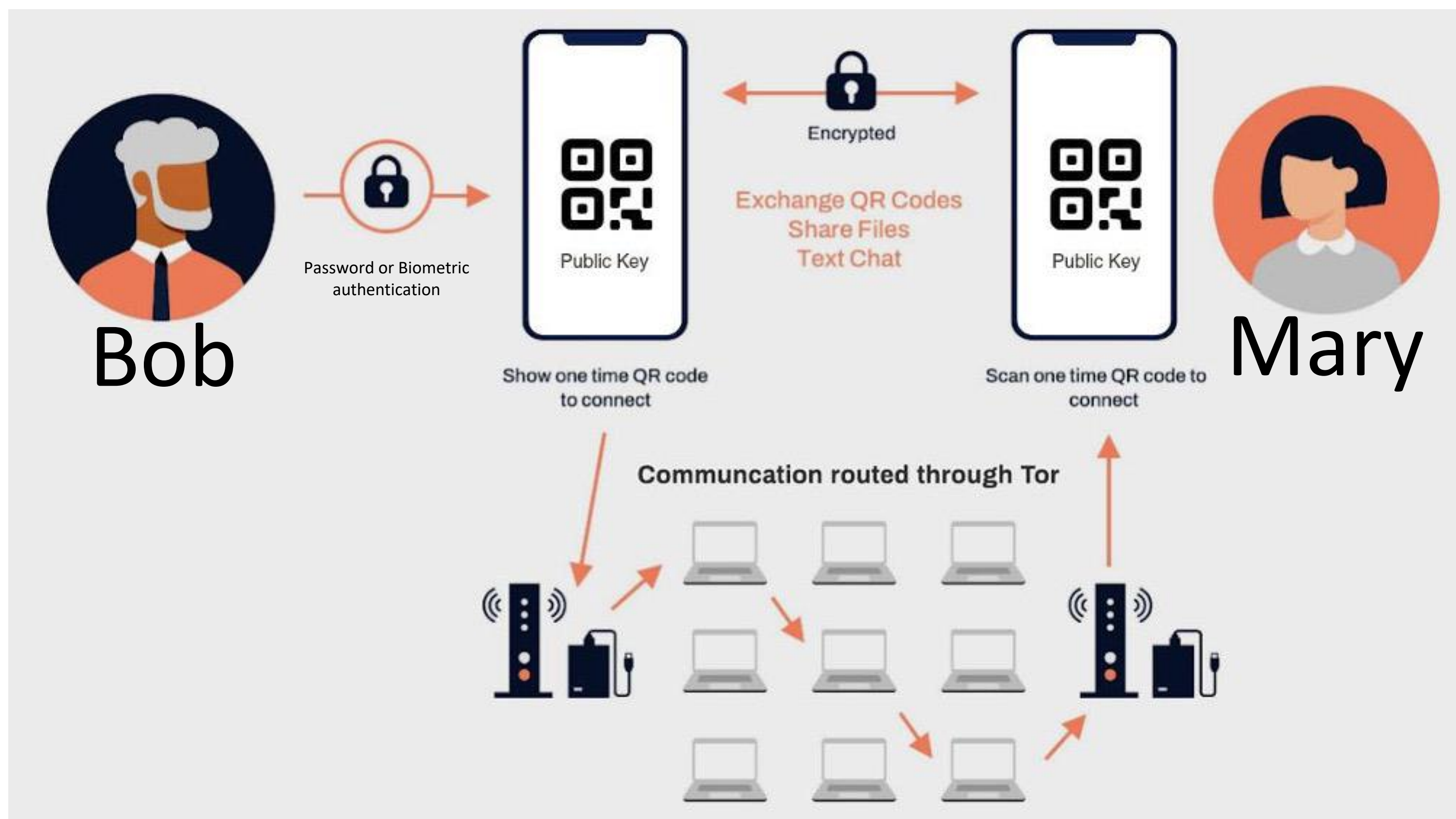
Figure 1: Interconnections between networks in Russia (red nodes) and other networks either inside or outside Russia. Networks outside Russia are blue nodes. Tier1 networks are green nodes.

How to bypass censorship and protect refugees privacy?

Create direct connections on a privacy-protecting, censorship-resistant and cryptographically-secure network.



The Solution - Direct, Mobile, Peer to Peer connections over Tor



Each individual connection is created, encrypted and stored at source. Individual network connections are stored on users' mobile devices, not in third party servers susceptible to surveillance or blocking.

For users subject to censorship, individual mobile 'containers' are connected to the Internet via Snowflake. [Snowflake](#): is an Internet access system designed to avoid censorship. Connections go through Snowflake proxies, which are run by volunteers.

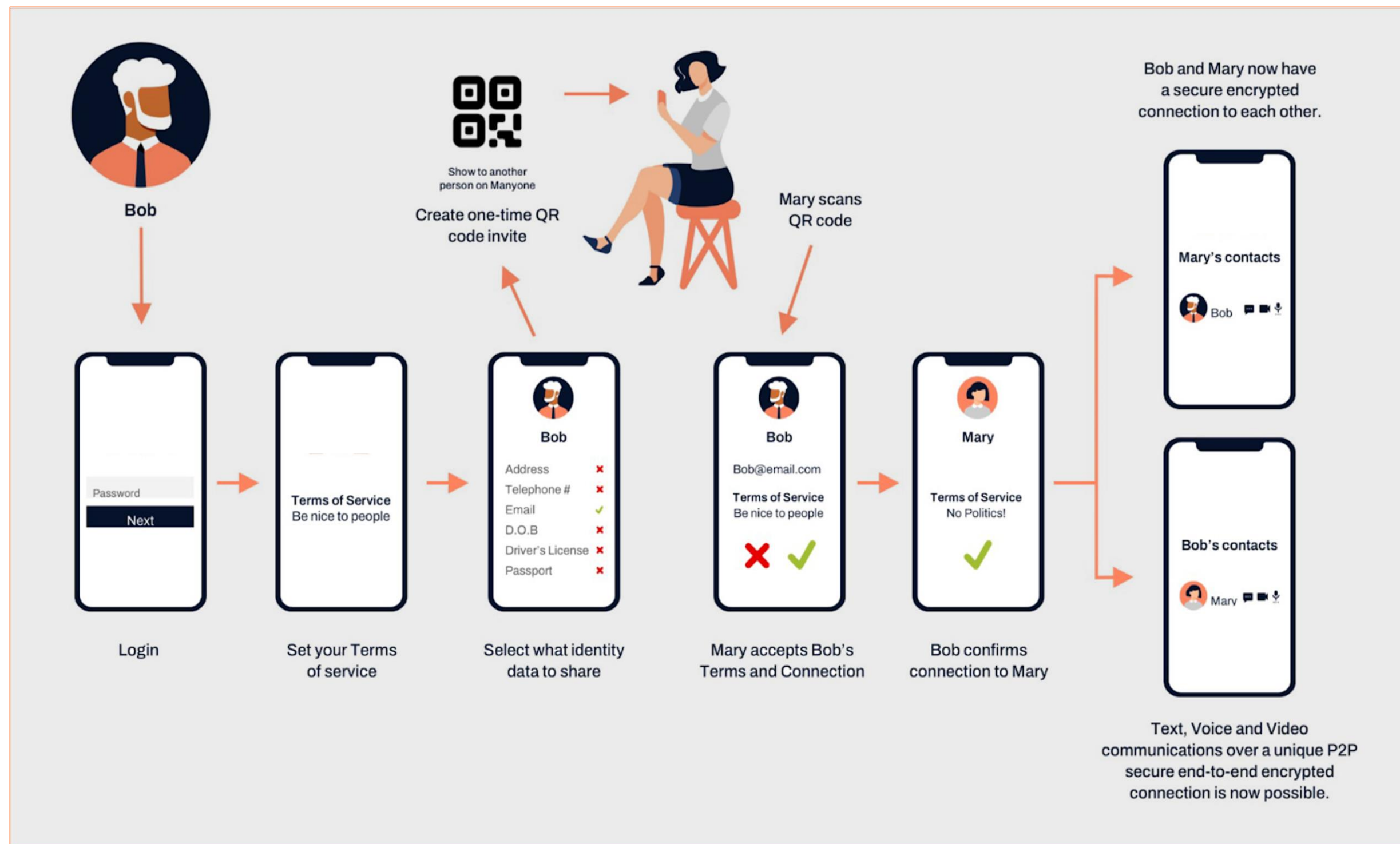
This ensures user connections from mobile devices cannot be tracked or easily blocked. For information about Snowflake, see their [documentation wiki](#).

Transmit messages, pictures & files over Tor:

[The Tor project](#): represents 30 years of effort to create internet connections that don't reveal who is communicating with whom, even during active network monitoring.

The design of the Tor network protects the privacy of its users and makes the task of preventing users from accessing the Tor network nearly impossible. The Tor Project channels substantial resources to ongoing research of new ways to allow its users to circumvent censorship by powerful state and non-state actors.

What's Next? - Create & Share Digital Identity Attributes



Decentralized, Mobile, Individually Controlled Digital Identity

Add a digital identity attribute claims 'container' to mobile Tor-based connected nodes

Create claim of identity attributes including:

- Name, address, telephone, email
- Citizenship, passport, health, birth certificate
 - Bank, KYC, credit card
- Land title, physical property

Share user attested identity claim attributes with other users over a P2P network whose design intrinsically resists tampering, censorship, and metadata analysis. (Snowflake via Tor)

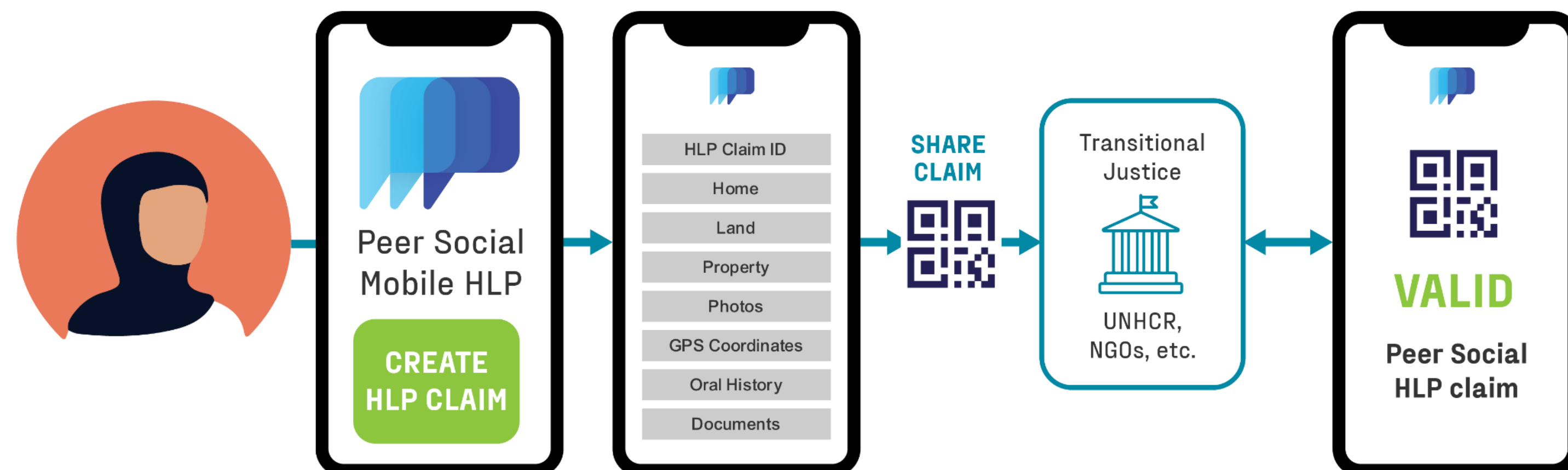
- Users can give and receive confirmation of shared individual identity attributes.

Digital identity attribute 'container' is portable and can be backed-up and stored anywhere a user chooses:

- On a user's smartphone
- On a shared physical server
- On a shared Cloud virtual server
- On a home-based network-connected hardware device

Use Case: Transitional Justice Home, Land and Property (HLP) for Ukraine

A supported, open-source Research & Development project to develop a *trusted* P2P mobile application to enable over 86 million refugees to document their existence for identity assertion, asset restitution or recovery under [Transitional Justice](#).



Requirements for trust by refugees and displaced:

- Decentralized - does not require a third party to broker connections.
- Mobile - all data and connections *only* in possession of the end-user.
- Robust - data and connections must be censorship and metadata-resistant to ensure trust.
- Archivaly Sound - Ensure that data is stored in an authentic, encrypted, decentralized, time-stamped and “hashed” tamper-resistant fashion so it cannot be viewed by hostile parties / governments.
- Accessible - Ensure that the record consists of photos, documents and audio & video attestations. Ensure that the contents of their record can be ‘published’ to a tamper-proof portfolio for review by third parties.

- Whitepaper: [Trusted Records in Tapestry Approach: A Background Study to Inform System Design](#)
- Podcast: [Why Decentralization Matters: A conversation with Transitional Justice analyst Dr. Jon Unruh.](#)
- Presentation: [Digitally Designed Housing, Land & Property \(DDHLP\)](#)



Dr. Jon Unruh, McGill University

Home, Land & Property (HLP) - The Problem and Solution



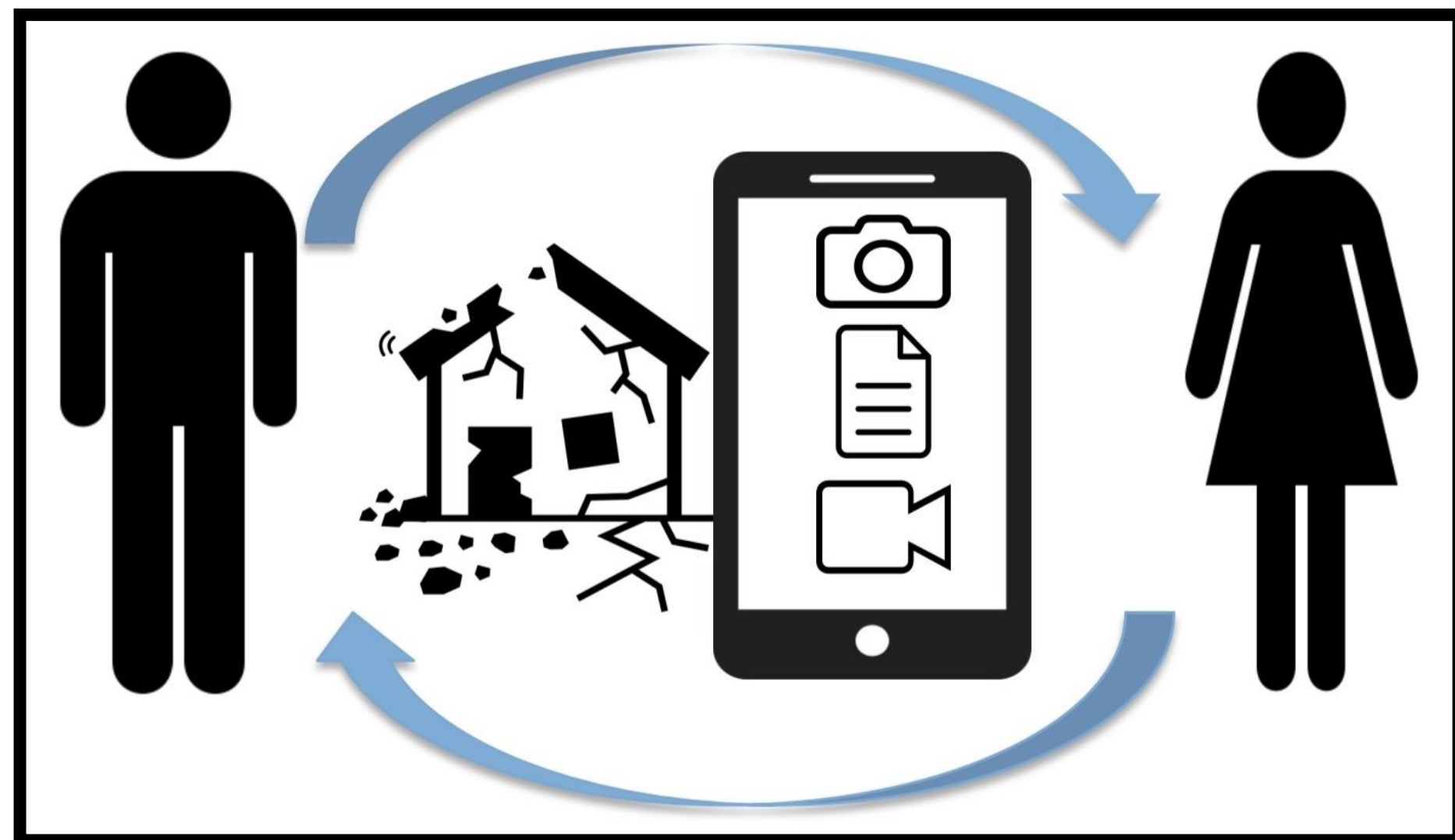
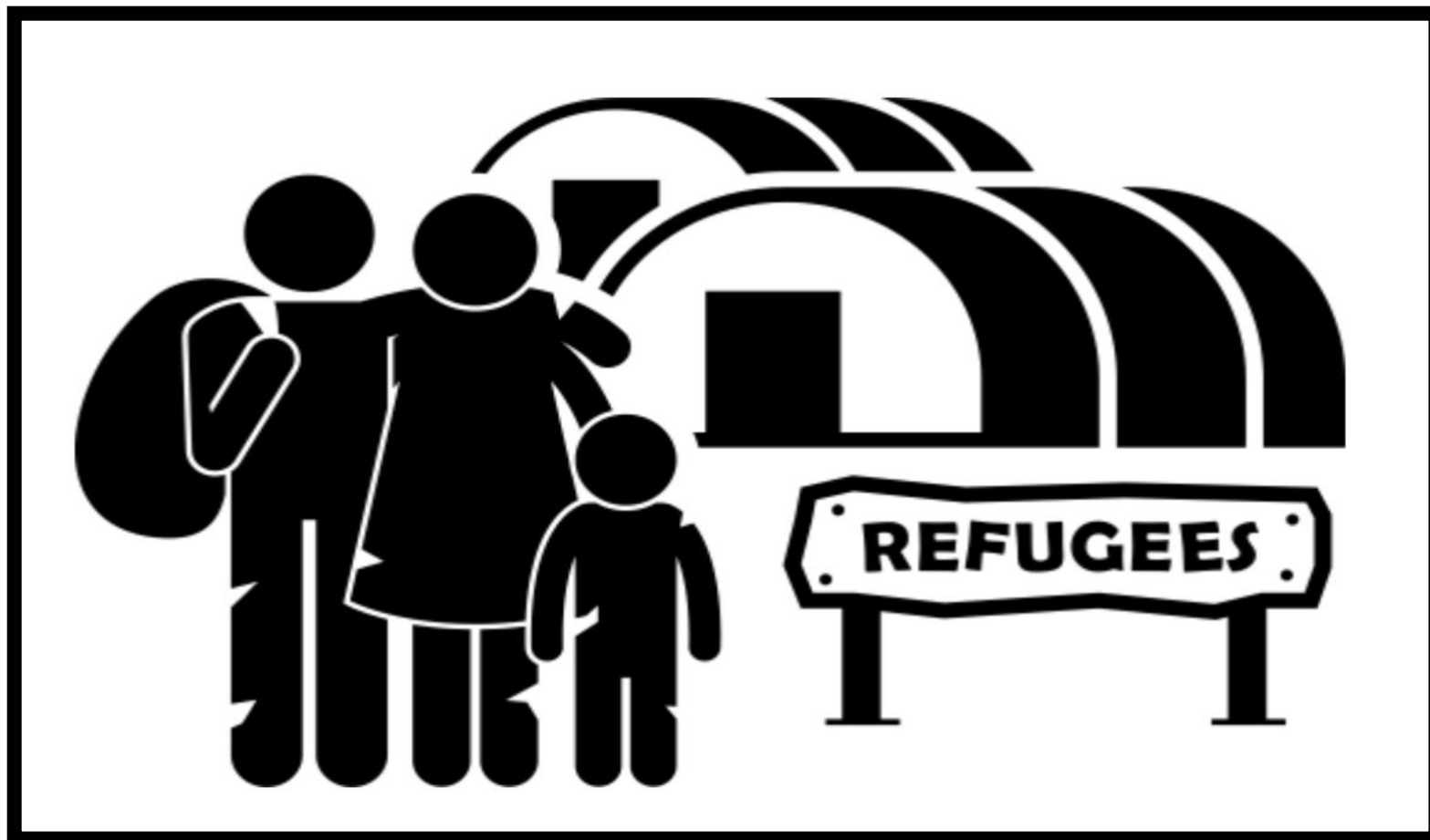
Past research has shown the need to move quickly in situations of mass forced population dislocation,

- So as to be able to effectively capture recognition & recollection of land and property 'evidence for claim', before they are lost.

Waiting until a war is over before establishing a program for how refugees will reclaim HLP is an expensive & very long process that:

- Marginalizes those who have lost important evidence over time,
- Results in a reluctance to return from refugee hosting countries.

Legalities, techniques & technologies for large-scale housing, land and property restitution/compensation programmes

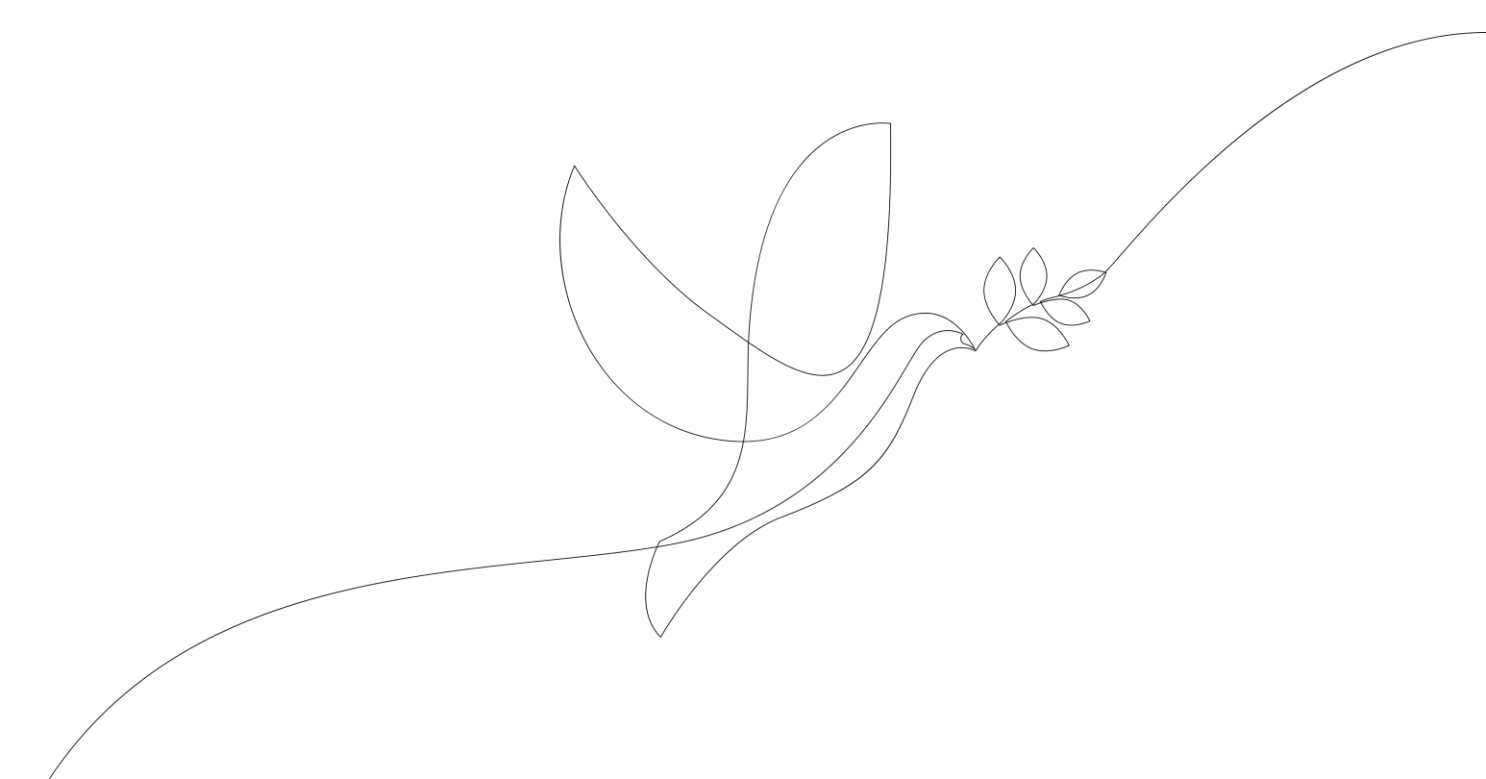


- No national legal/institutional process designed for stable settings can manage the influx of hundreds of thousands to millions of HLP claims in a war-affected setting.
- There is widespread loss of HLP documents as people: flee; destroy them to prevent confiscation and use in ethnic cleansing, expropriations, trafficking and military targeting; or lose them in destruction, duress and coerced sales—if documents ever existed.
- Alternative evidence for claim — dislocated populations usually do not know what evidence they have, or can obtain.
- The UN best practice for HLP restitution—mass claims and transitional justice—***urgently needs a tech upgrade.***

The legal techniques for HLP mass claims & transitional justice are well established



- What is needed is to be able to apply these techniques in a much quicker, low cost, larger-scale way.
- Current technologies can provide this



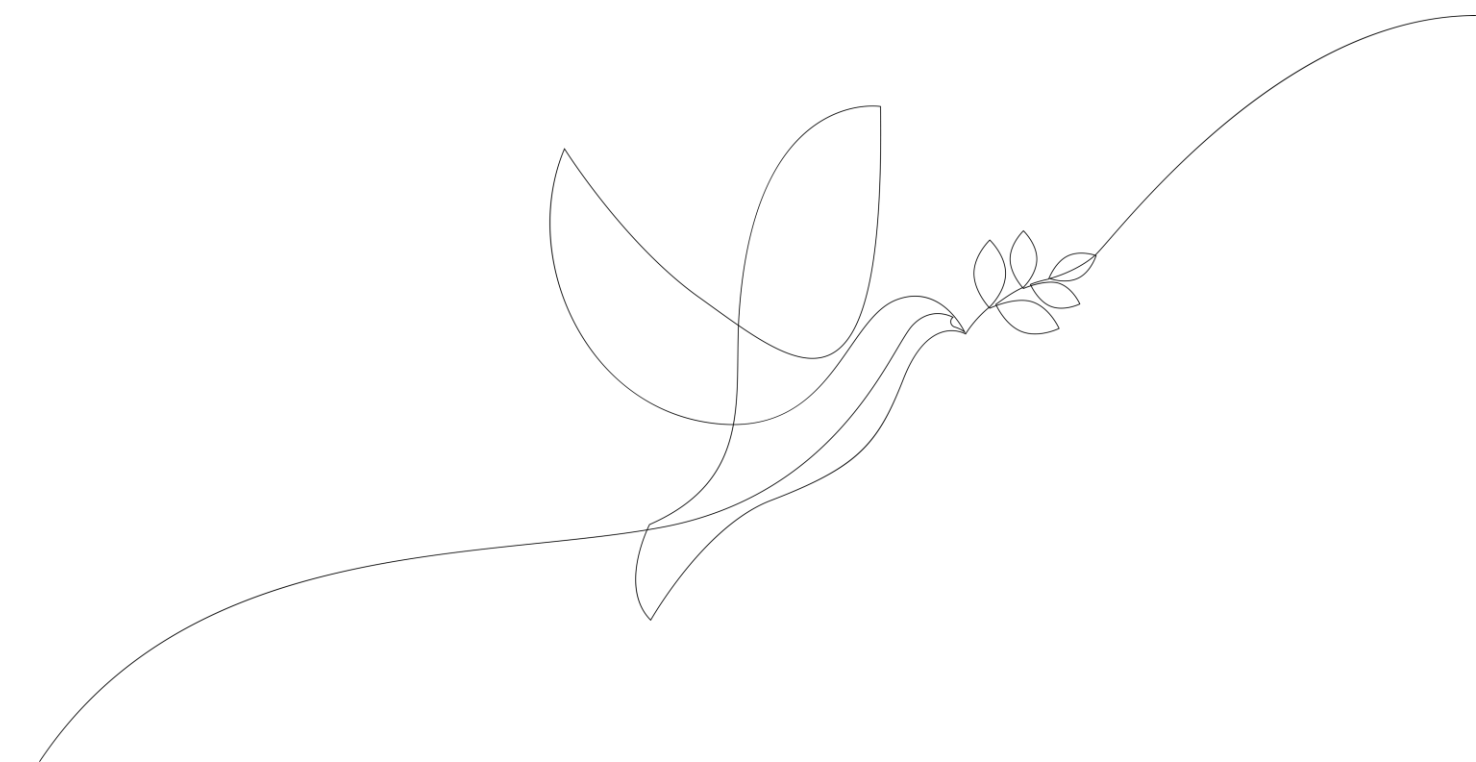
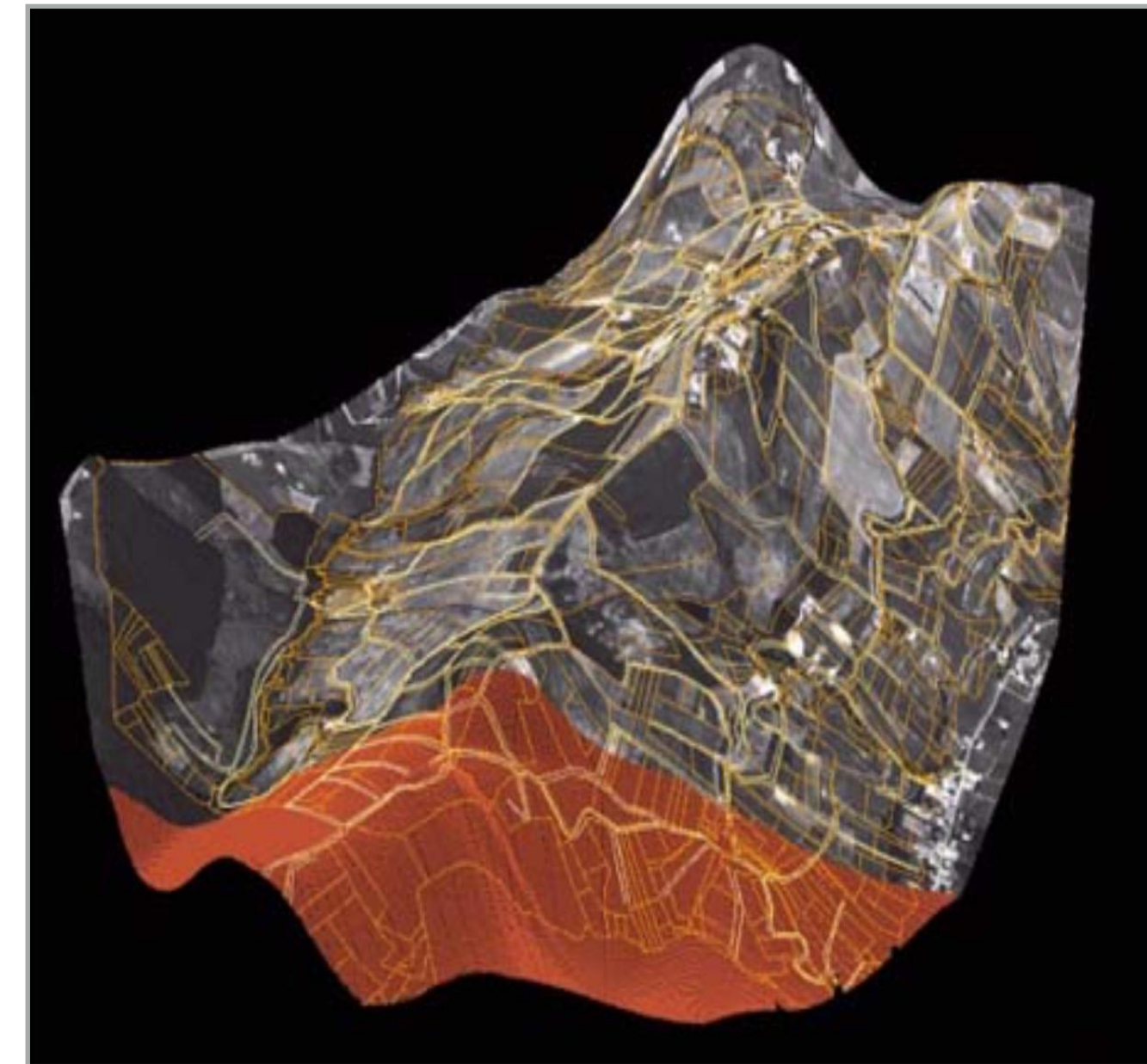
Example: Database Construction

Issue: Database needed for claims processing techniques

- Needed for categorization, legal decisions, assigning remedies,
- Data entry for claims usually takes place after the war,
- Time consuming, costly,

Upgrade

- Refugees enter their own claims information with an app:
 - 'Fit for purpose', user-friendly, varied levels of literacy, wide variety of data types: (audio, photos/video, text, hand drawn maps)
- Does not wait until after the war for database construction,
- Cost is greatly reduced.



Example: Real-Time Collection of Evidence

Issue: Obtaining new evidence

- Historically not possible for dislocated populations

Upgrade

- Most refugees from Syria, Iraq & Ukraine communicate with friends & relatives back home - by mobile phone.
- This allows additional evidence to be gathered - photos & video, location (descriptive & GPS), testimony,
- For further corroboration.

How Do the Syrian Refugees Communicate with Their Relatives in Syria?	In Camps			Out of Camps		
	Male	Female	Total	Male	Female	Total
Mobile Phone	87.7	88.2	87.8	89.3	86.4	88.6
Fixed Phone	1.1	0.6	1.1	1.6	1.0	1.5
Internet	8.7	8.1	8.6	5.7	6.8	5.9
Letter	0.5	0.0	0.4	0.6	0.0	0.5
Other means	2.1	3.1	2.2	2.8	5.8	3.5

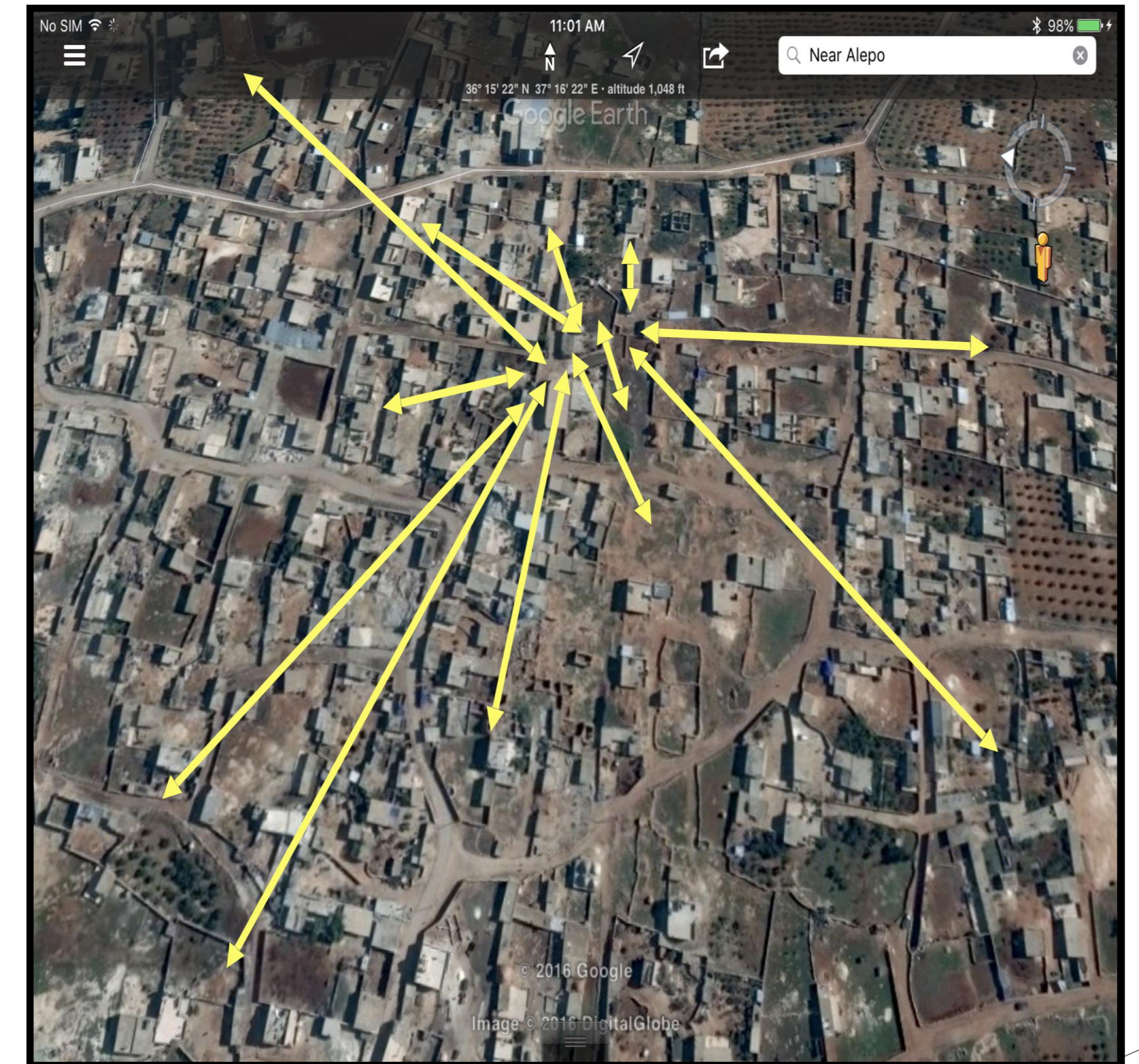
Example: Evidence - find your neighbours?

Issue: Corroboration of boundary claims by neighbours

- Historically not possible for dislocated populations

Upgrade

- Use of phones, social media to locate relatives & neighbours (even if scattered in different countries),
- Agreed upon boundaries between neighbours as valuable evidence,
- Creates a spatial network effect of boundary corroboration,
- Not just adjacent neighbours, but other neighbours, friends & relatives nearby who can also attest to boundary location & and who was the owner/occupant.



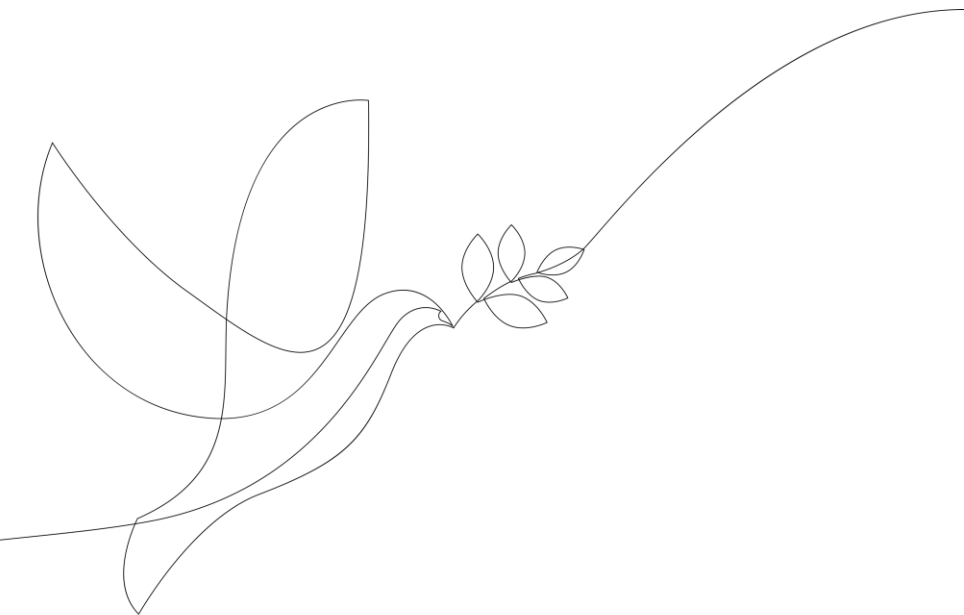
Example: Matching - Evidence Corroboration (non-party evidence)

Issue: Corroborate claims with data in other databases:

- Electricity, water, school, neighborhood, associations, etc., containing related facts of presence, residence, occupation, etc.
- Very difficult in times of war to access such in-country databases.

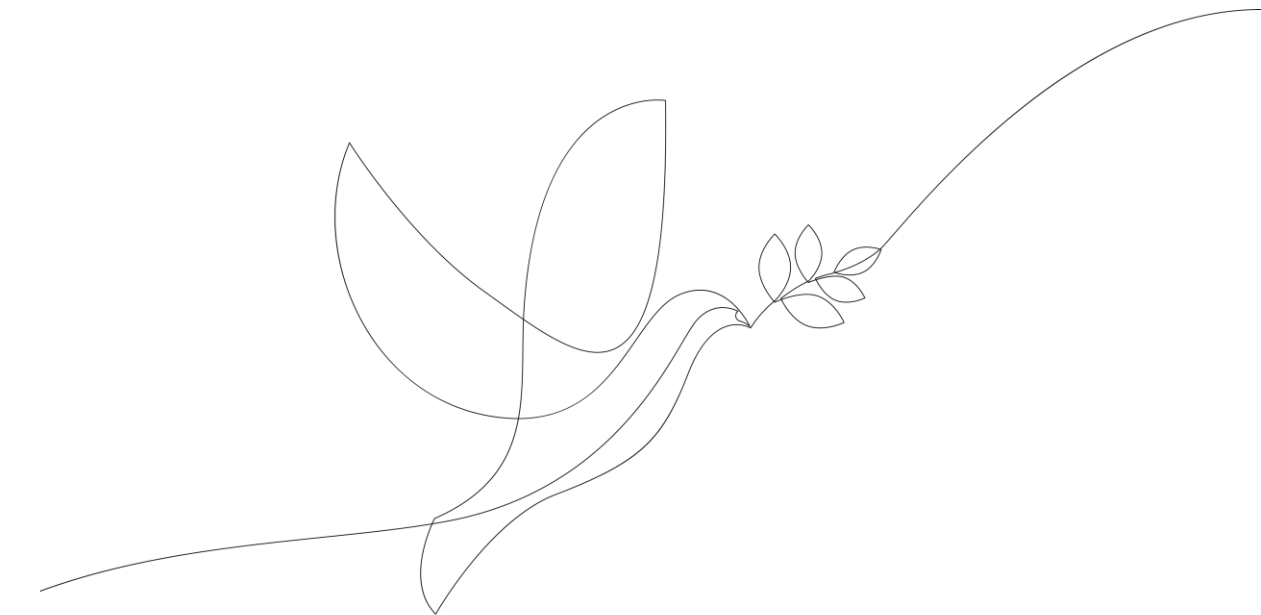
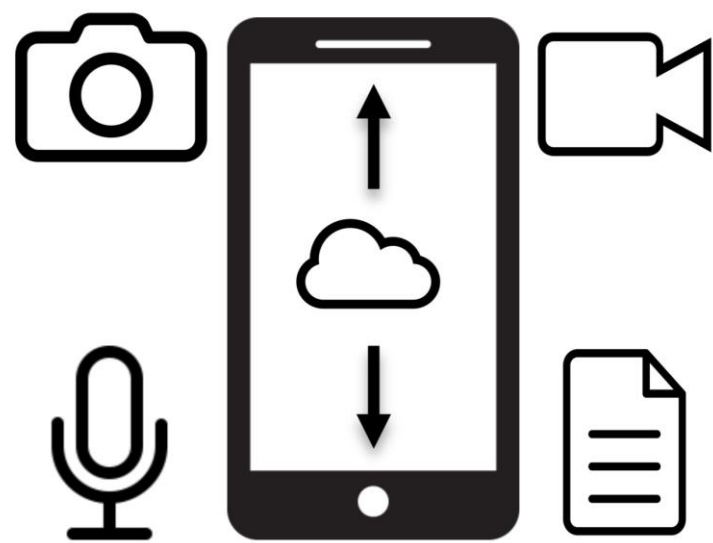
Upgrade:

- Internet data - instead of national databases, for corroborations in time, space, events;
- National and international databases, social media, news reports, satellite imagery, data mining, etc.
- Evidence corroboration can occur automatically.



Many conventional legal techniques for mass claims resolution for war-dislocation can be upgraded

- No new legal work is needed for resolving claims;
- Upgrades a paper-based approach, standing in long lines to file claims (usually men only), then data entry - costly, time consuming;
- Upgrades allow for claimants to be anywhere, male or female, data entry phase is skipped, categorization begins immediately;
- Ultimately, in order to use funds for reconstruction of civilian HLP, claims must be filed, decided, and remedies implemented.





Dr. Victoria Lemieux

**SAFEGUARDING THE RECORDS OF HOMES, LANDS, AND PROPERTY FOR
DISPLACED PEOPLES FROM CONFLICT-AFFECTED AREAS**



Guardians of the Record Lab – who are we?

- The Guardians of the Record Lab conducts research on capturing, maintaining and protecting the authenticity and integrity of records in human rights contexts.
- Our current project explores the unique challenges faced by persons displaced by conflict in relation to safeguarding records of their abandoned homes, lands, and properties.

"protect the record so that you can protect the people"



Graduate Students



**Panthea
Pourmalek**

Master of Public Policy and
Global Affairs



**Niloufar Vahid-
Massoudi**

Master of Public Policy and
Global Affairs



**Samantha El-
Ghazal**

Master of Public Policy and
Global Affairs



Nicole Johnston

Master of Public Policy and
Global Affairs



Amber Gallant

Master of Library and
Information Studies



Hoda Hamouda

Ph.D, Library, Information,
and Archival Studies



About the survey- our sample

- We limited the geographic distribution of our survey to four regions that are currently experiencing either active or protracted conflict. We further subdivided these regions into ten countries, all of which are experiencing an active or protracted conflict, or type of violence.

Latin America

- Mexico
- Colombia
- Guatemala

Eastern Europe and South Caucasus

- Ukraine
- Georgia
- Moldova

Middle East

- Yemen
- Syria
- Lebanon

China

- Xinjiang

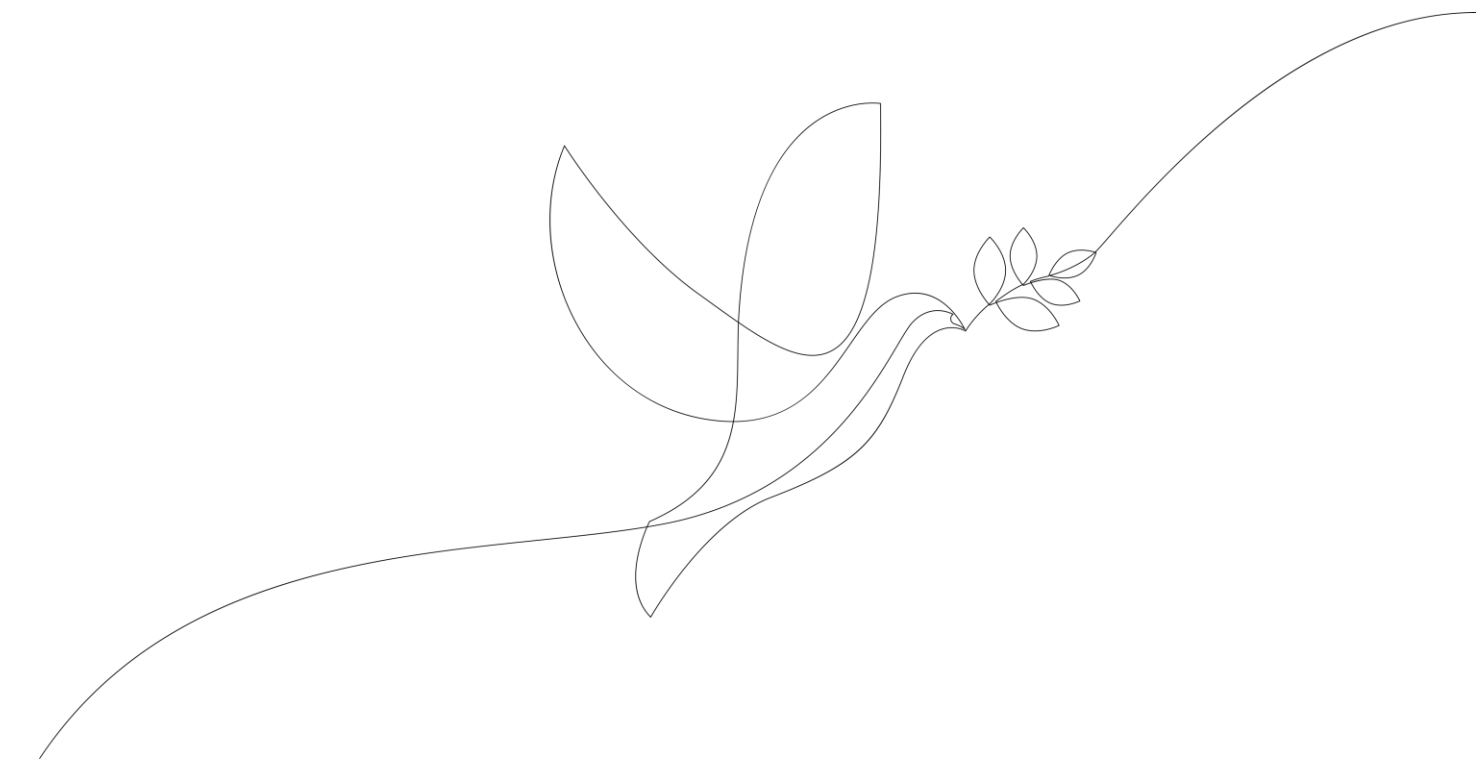


About our survey - Types of Questions

The survey is divided into four parts:

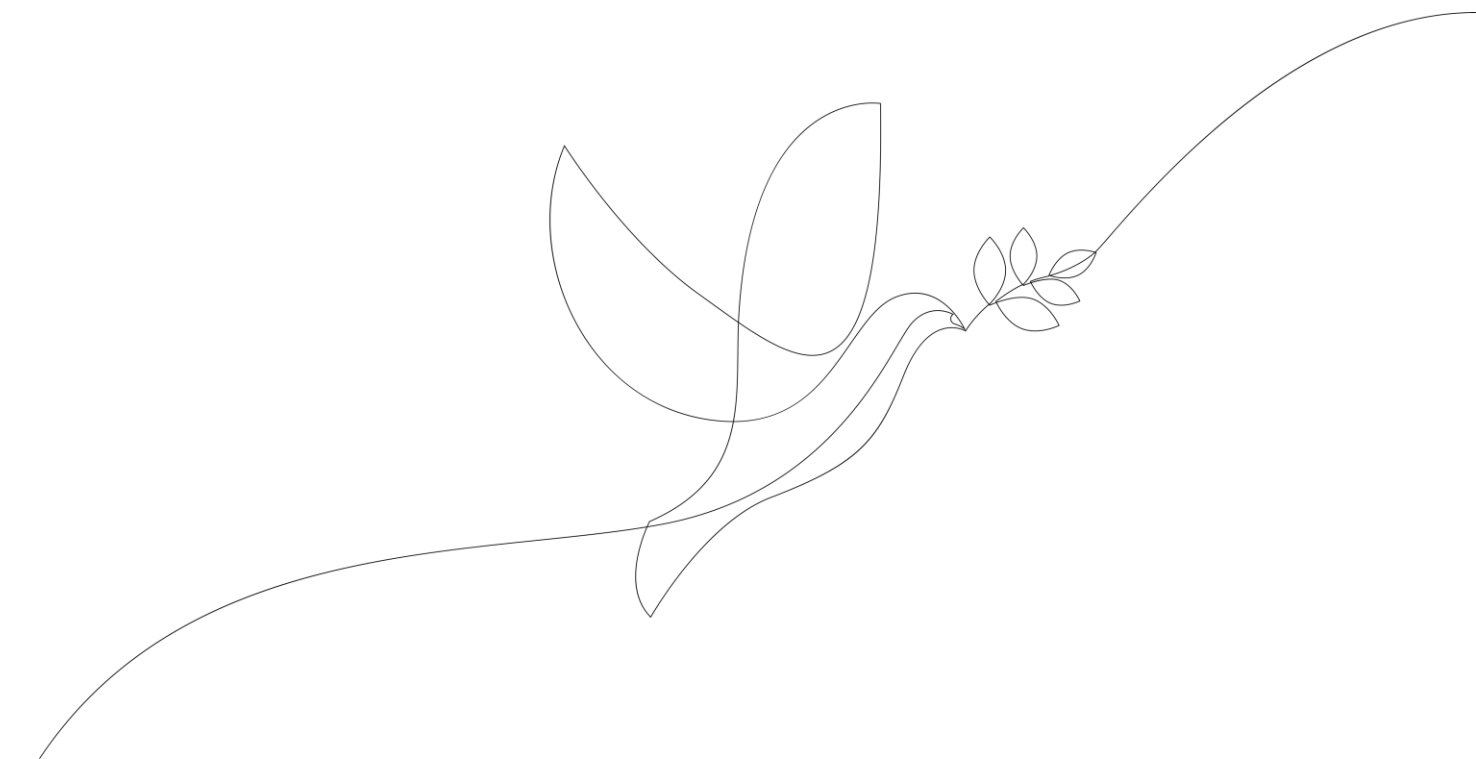
Part 1: Background information about organization

- Mission
- Funding
- Country(ies) served
- Years in operation
- Primary beneficiaries



Part 2: Archival focus of organization

- What purpose archival work serves
- What kinds of information are created, captured, preserved and/or verified
- External guidelines used in establishing archiving process
- Tools and databases used in archiving process



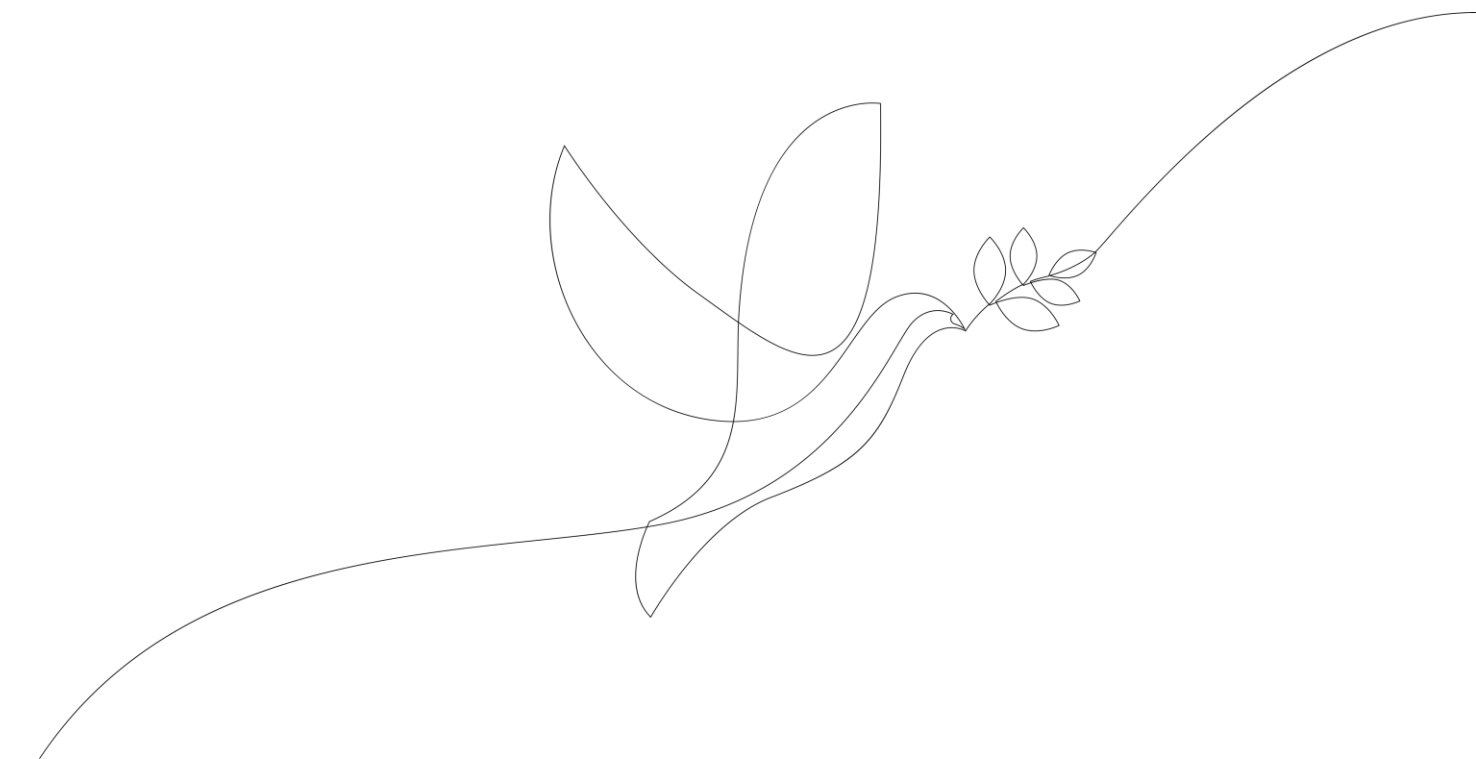
Part 3: Experiences in using archival tools or practices to create documentation

- Practices used to ensure the authenticity and integrity of records
- Gaps or challenges in protecting authenticity
 - Verification of authenticity
 - Longevity and sustainability of evidence
 - Personal or organizational safety or security
 - Scaling up of archival operations
- Sufficient experience and knowledge to fulfill mission and operations



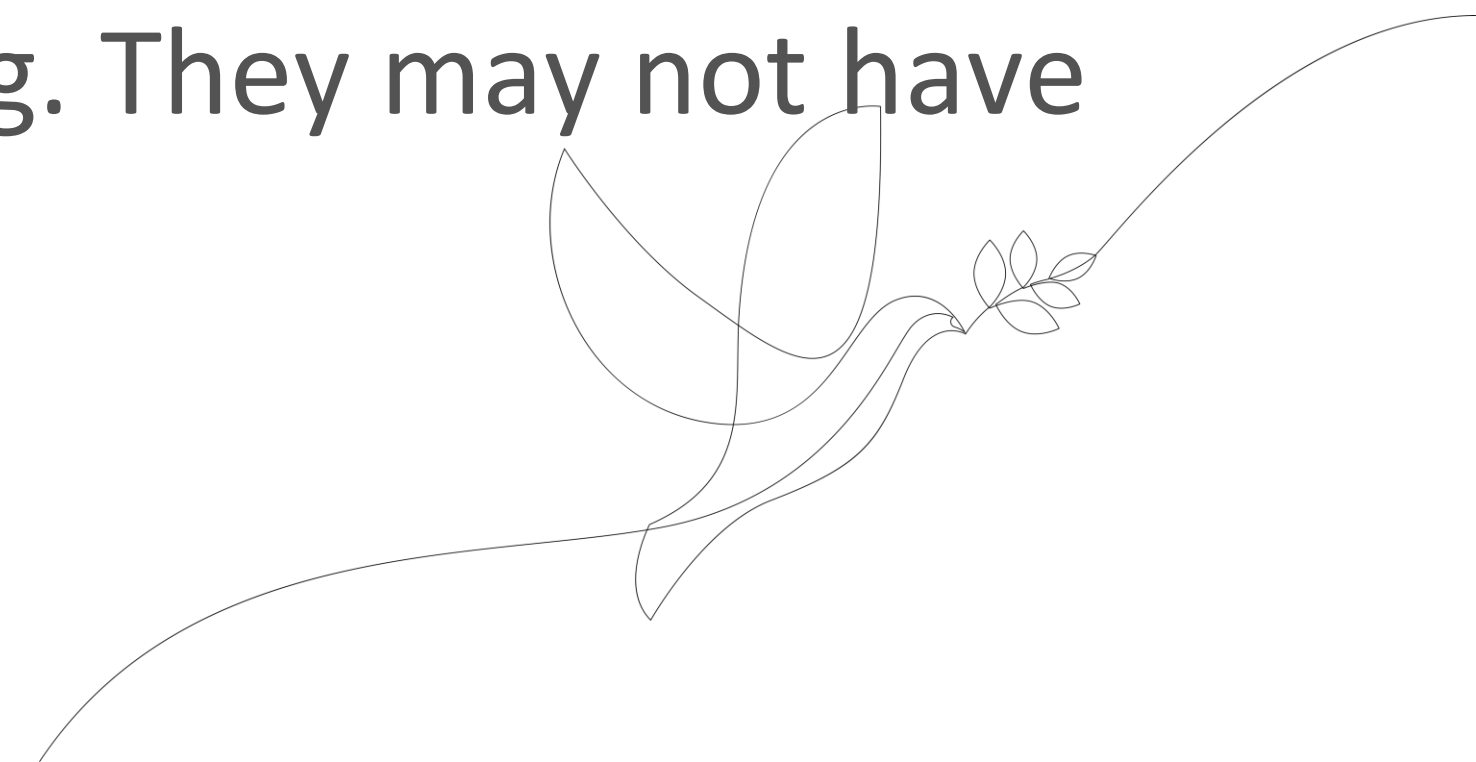
Part 4: Perception of archival work within and without the organization

- How organization works to build trust needed for collection of information
- Sharing of information for transitional justice purposes
- Challenges in admissibility and authenticity of evidence

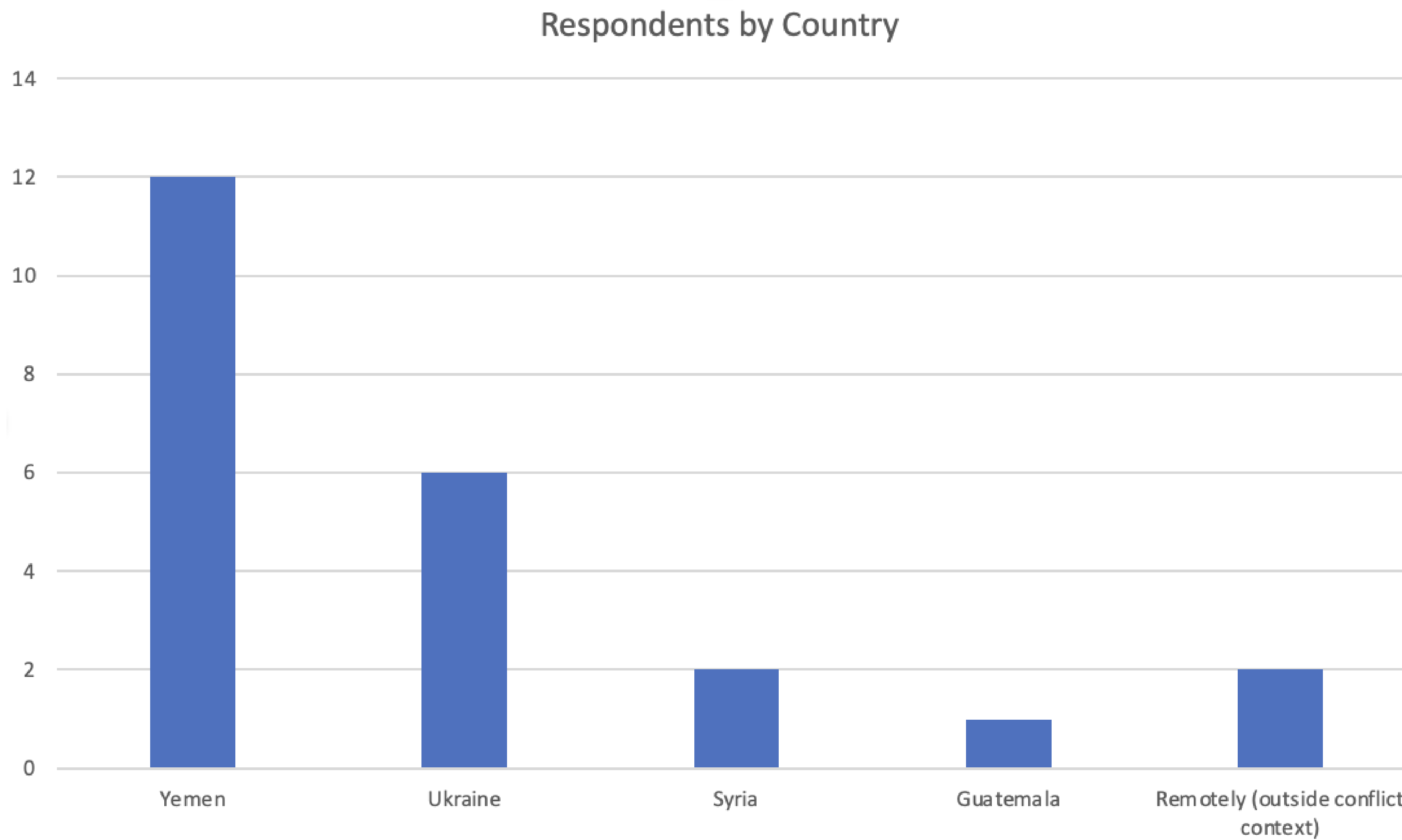


Survey results

- We received 22 complete or partial responses to our survey.
 - 13 from Yemen
 - 6 from Ukraine
 - 2 from Syria
 - 1 from Xinjiang (operating remotely)
- The response rate reflects the fact that organizations operating within conflict contexts are already stretched in terms of staffing and funding. They may not have ability to take on extra work.

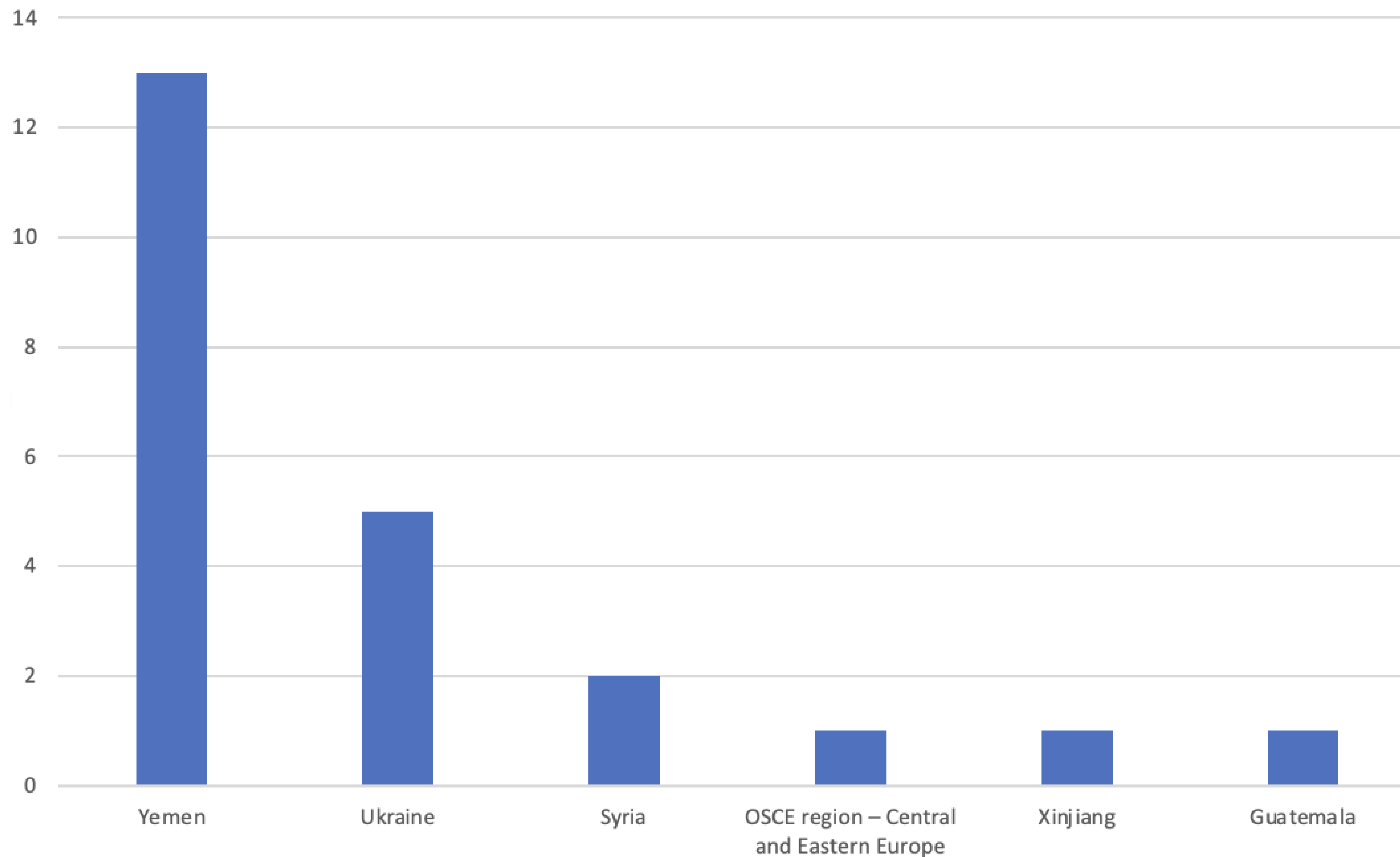


Survey Results – Breakdown of respondents by Country



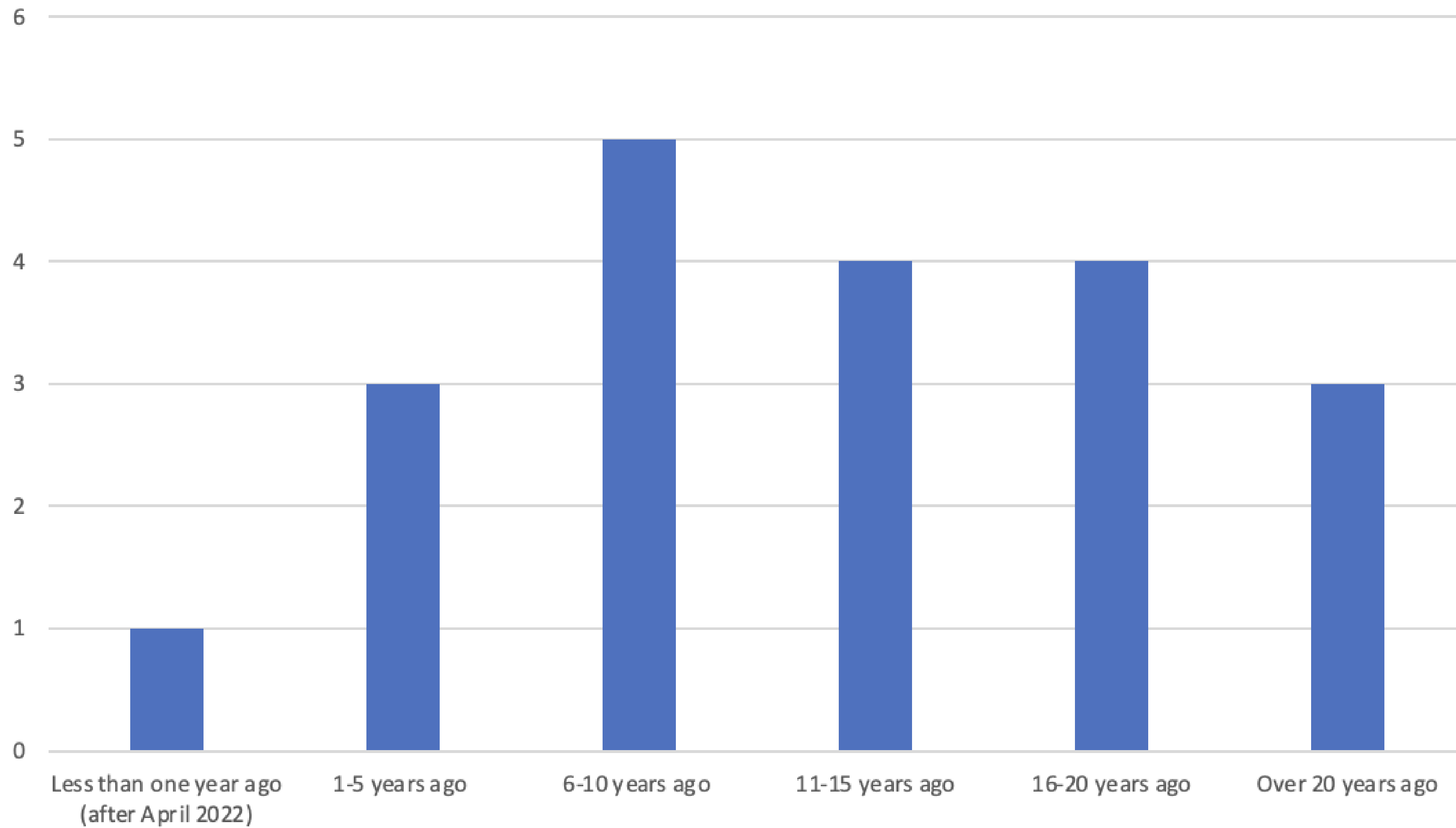
Survey Results – Breakdown by Country of Focus

Focus of organization



Survey Results – Time in Operation

Establishemnt of organization

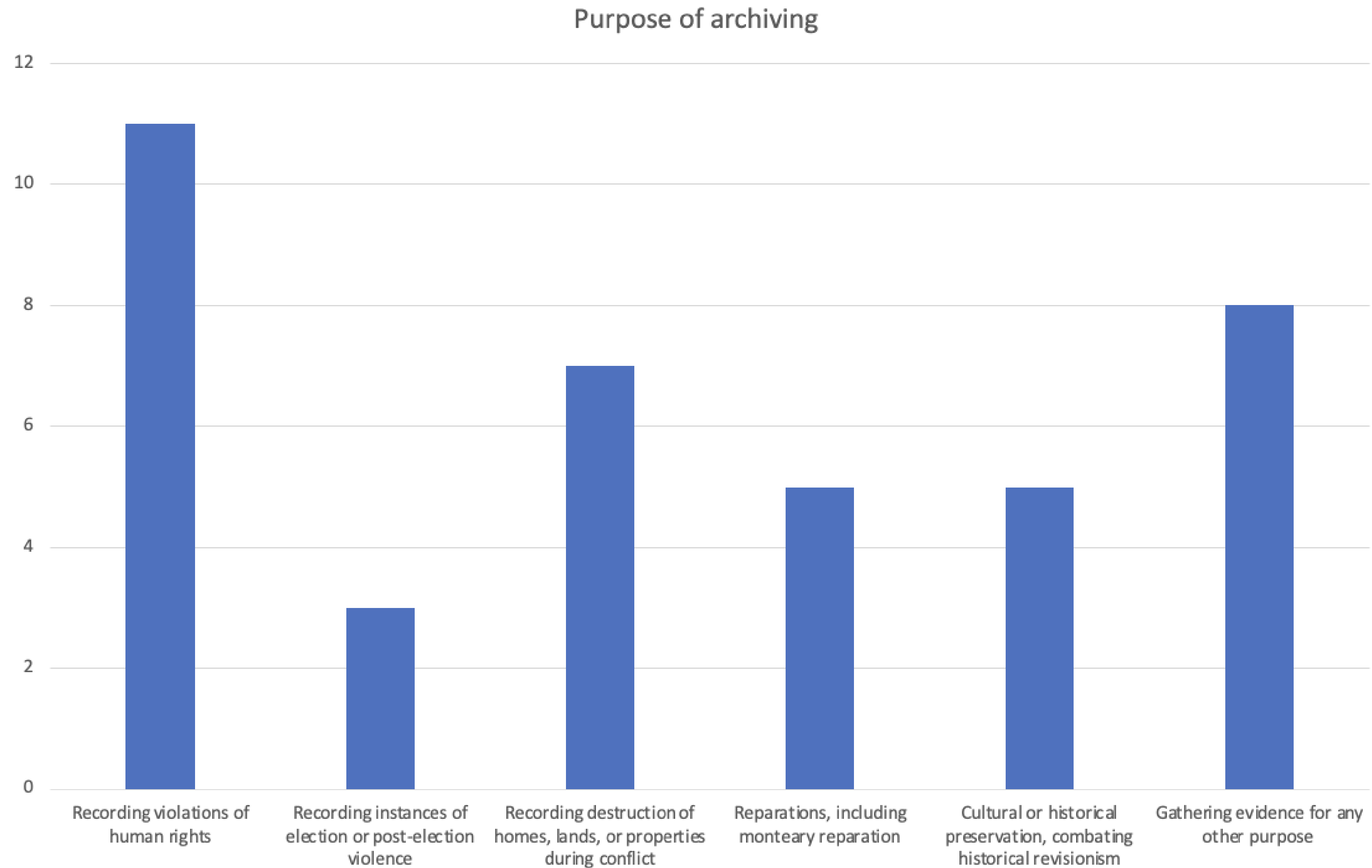


Survey results – Mission of organization

- Survey results – Mission of organization
 - “[to] reinforce the concepts of peace and coexistence...”
 - “Stimulating community participation in peacebuilding...”
 - “mobilize efforts and advocacy to enhance cooperation and joint work with donors and international and local institutions in order to protect the lives of those affected during disasters and humanitarian crises...”
 - “[to] create a unified register of video and audio evidence of war in Ukraine...”
 - ”to document human rights violations in Syria...”

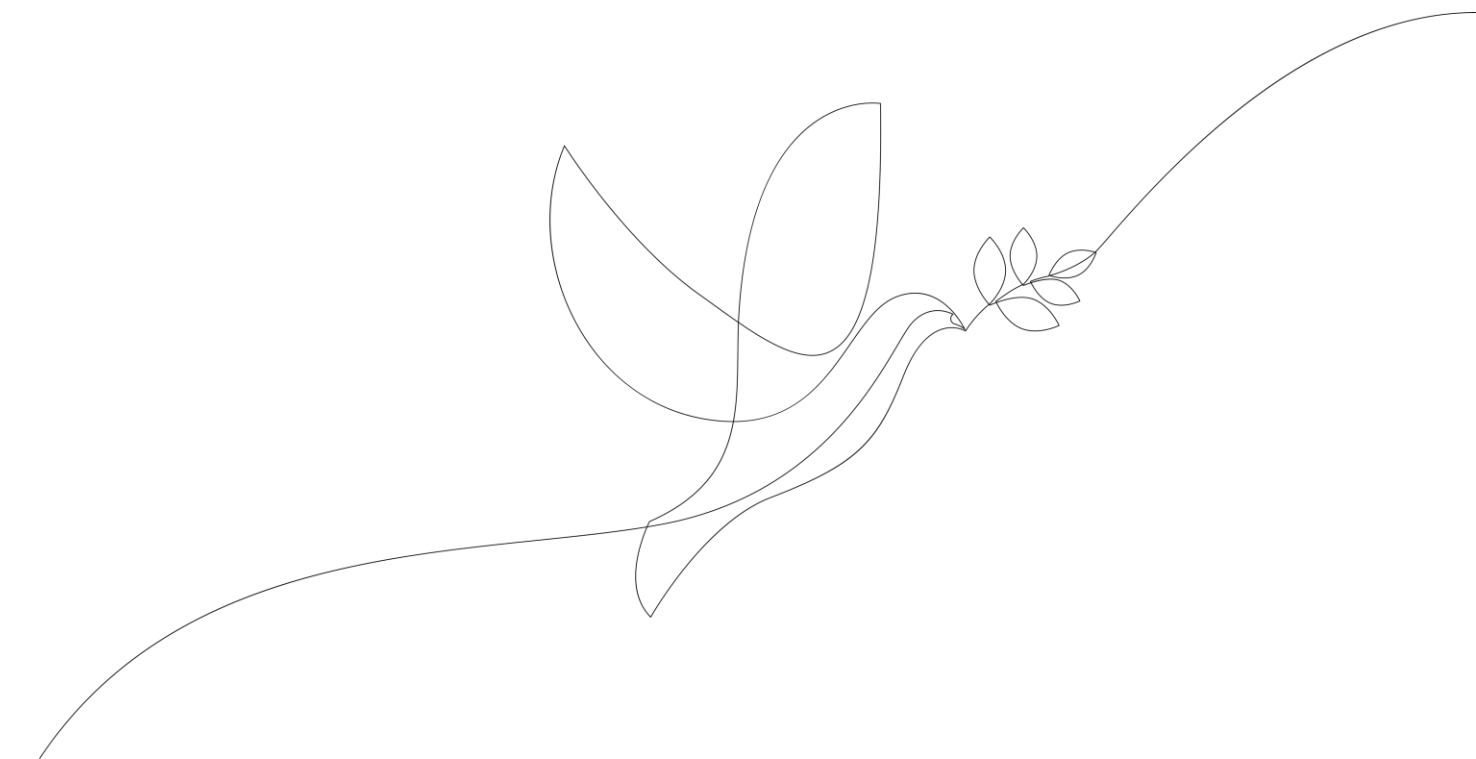


Purpose of Archiving



Types of Information Created, Collected, Preserved, or Verified

- In support of archiving for these purposes, organizations commonly worked with individual copies of land rights titles, digital copies of cultural materials, and videos/photos documenting human rights protests.
- They also indicated a range of other materials created, collected, preserved, or verified, including:
 - Radio clips and dialogues
 - Testimonies of war crimes collected from eyewitnesses (oral, written, official documents) - both on paper and written
 - Information related to organizational projects and activities
 - Documents or records preserving identity and collecting information about the situation of specific victims



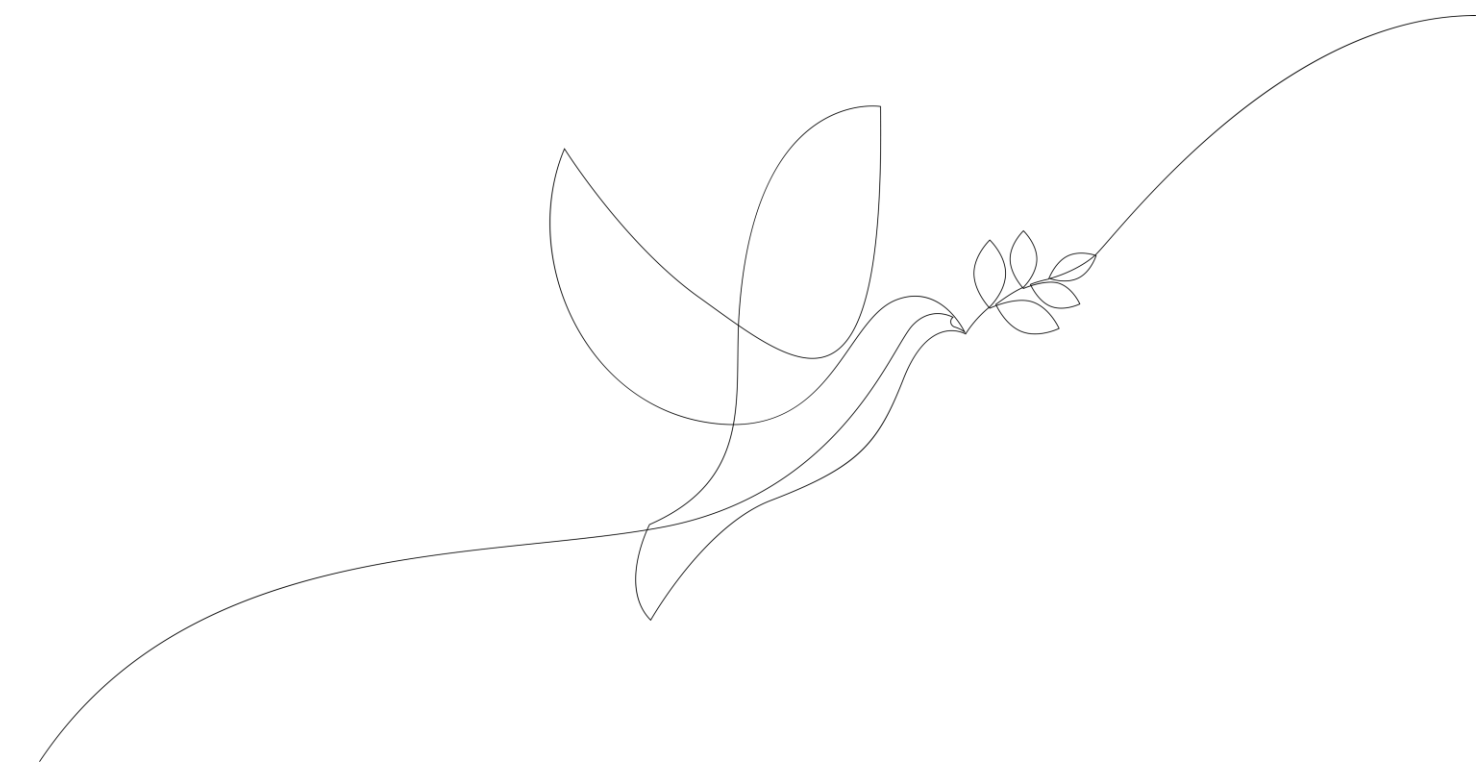
Modalities of archiving

- We asked, "If your organization is currently conducting archival work, or has done so in the past, how do you preserve and safeguard the records you have created and/or collected?"
- Organizations responded with a variety of tools and processes used in the preservation and safeguarding of their records. These included :
 - Hard disks
 - Emails and other digital formats
 - Clou services, including Dropbox or Google Drive
 - Secure physical or digital locations, left unspecified
 - A private database
 - Verification and preservation through reconstruction of original sources



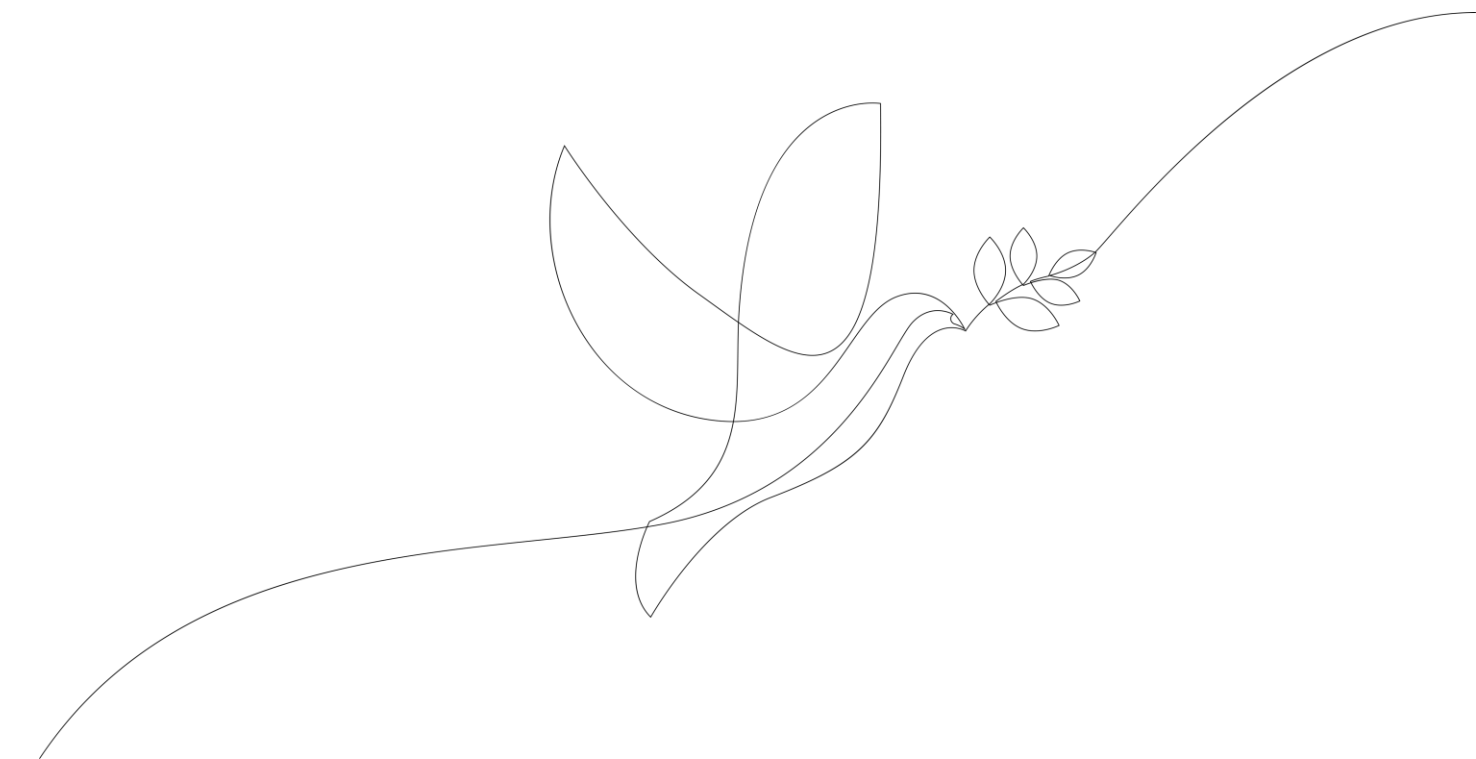
Usage of external guidelines Or archiving experts

- Though a wealth of resources resides with groups that build capacity for and provide expertise in archiving during conflict contexts (including Bellingcat, Ushahidi, HURIDOCS, and Khazaeen), only one organization indicated that they had reached out to any of these groups to establish archival practices. Another indicated that they had asked sectoral groups for guidance.



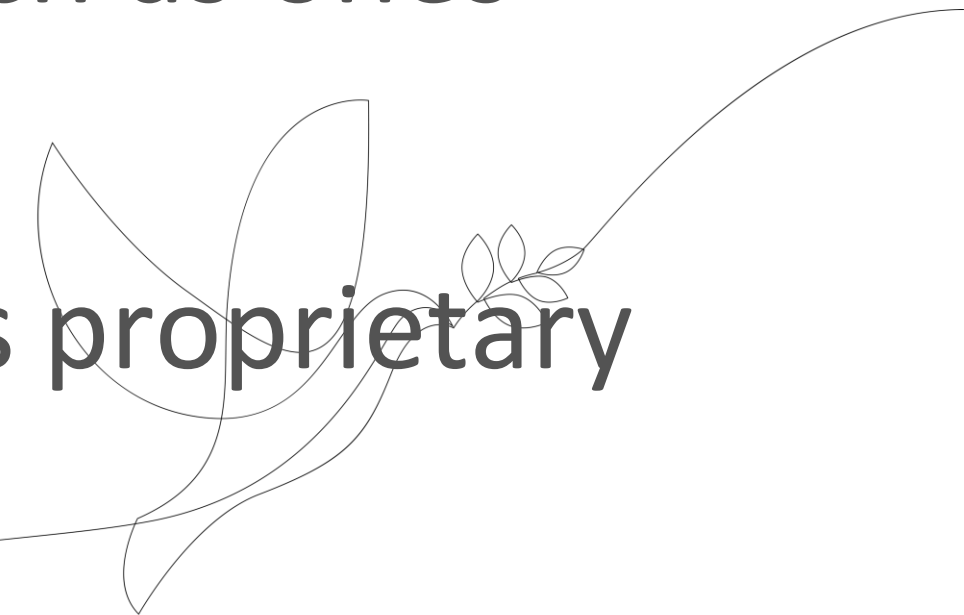
Conceptualization of authenticity

- We asked, “what practices do you use to ensure the authenticity of these documents (that they are free from tampering or corruption and that the document is what it says it is)?”
 - No steps are taken
 - Making multiple copies of records or hard drives
 - Physically inspecting documents for damage
 - Ensure documentation is created according to best practices and standards
 - Relying on trusted sources
 - Corroboration for verification
 - Track changes for MS documents



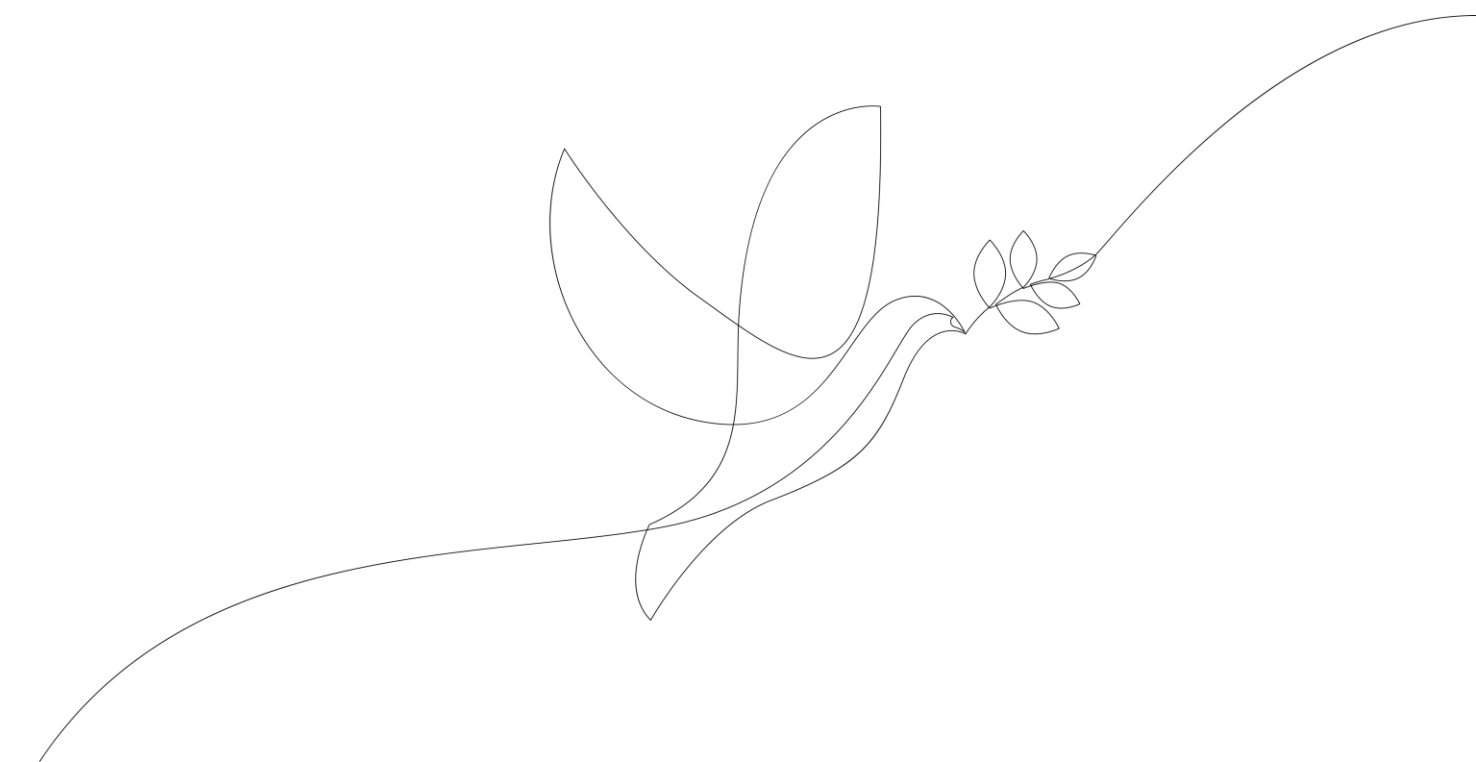
Gaps and challenges in the protection of records

- We received responses from 10 organizations on the types of resources they would like that they do not currently have access to.
- In terms of guidance notes, organizations desired information on:
 - Archiving
 - Data security
 - Data preservation for documentation concerning human and media rights in conflict contexts
- They also indicated that access to advisors and specialized programs (such as ones run by Swisspeace or WITNESS) would be helpful.
- A huge concern is funding. Without funding, organizations cannot access proprietary specialized tools nor fund the implementation of such guidance or tools.

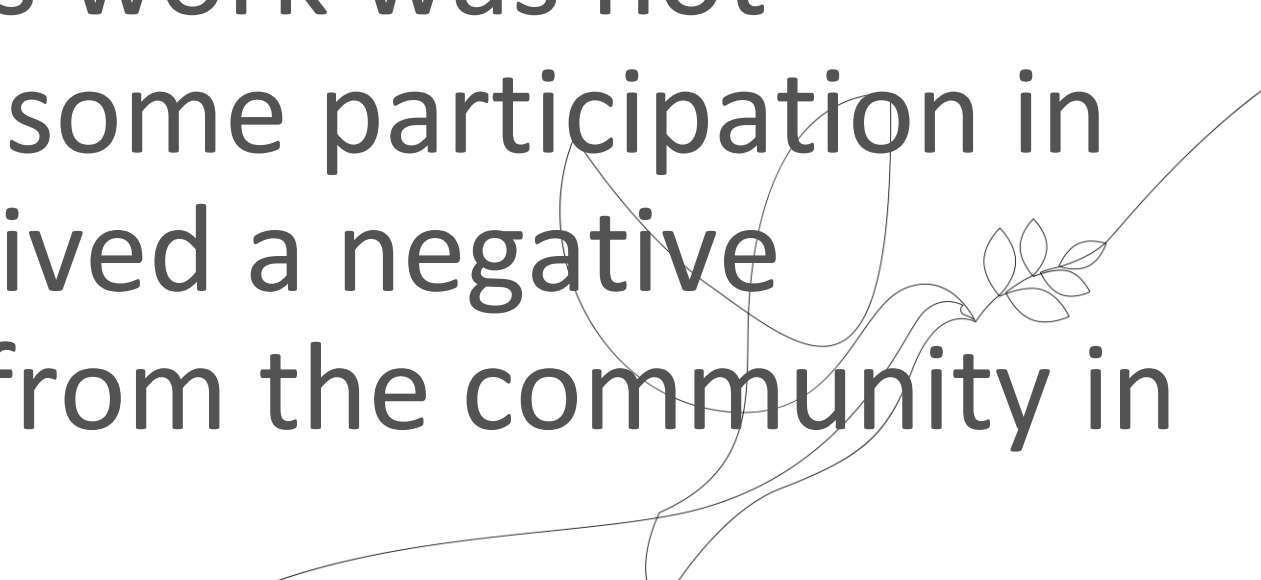


Reception from Community being archived

- How have communities worked to build the trust needed for collection of such records?
- We received 10 responses to this question, which revealed a variety of strategies.
- Building on relationships from past projects
- Relying on the reputation of the organization
- Taking steps to ensure proper coordination of efforts
- Being transparent
- Avoiding taking a political stance
- "Traditional methods"
- Still need to gain trust (one respondent)

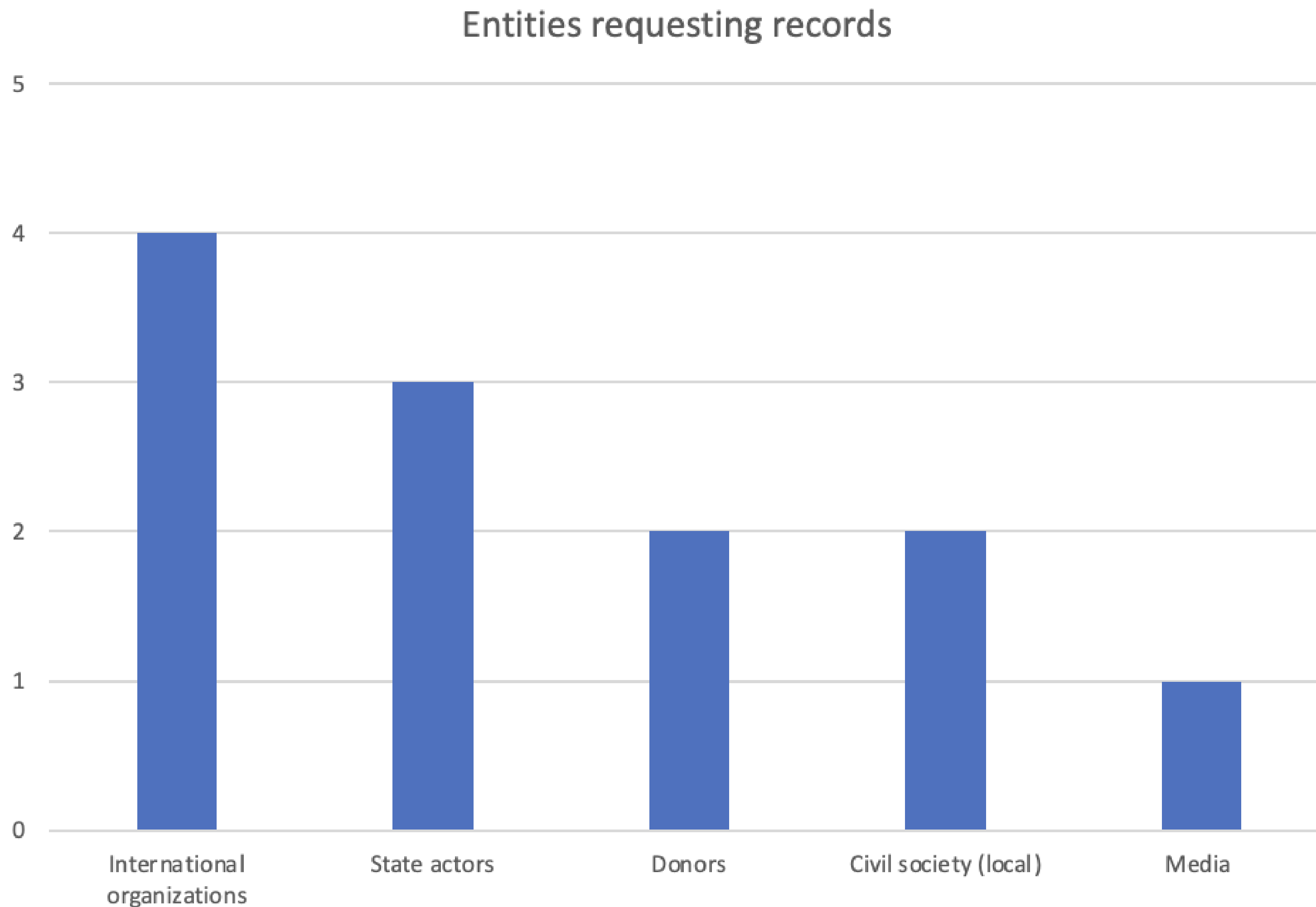


Reception from the Community Being archived

- Do you think that your organization's target community is willing and/or enthusiastic to participate in your organization's archival work?
 - Seven organizations indicated that they thought their community was willing and enthusiastic about participating in archival work; five organizations thought that the community was NOT enthusiastic about participation.
 - Would you say that your organization's target community views your organization's archival work as valuable and/or needed?
 - Only five organizations indicated that they thought the community viewed their work as important. Seven indicated that the community thought this work was not valuable or unneeded, suggesting that even though there was some participation in archival work, they hadn't collected specific feedback or perceived a negative perception from the community. There was specific feedback from the community in only four cases.
- 

Admissibility and reception from international community

Which entities have requested your records?





Dr. Geoffrey Goodell

Digital Payments for Compensation and Restitution Programmes



Of course, it depends on the design. A good design:

(1) Provides a **centrally-issued electronic token**:

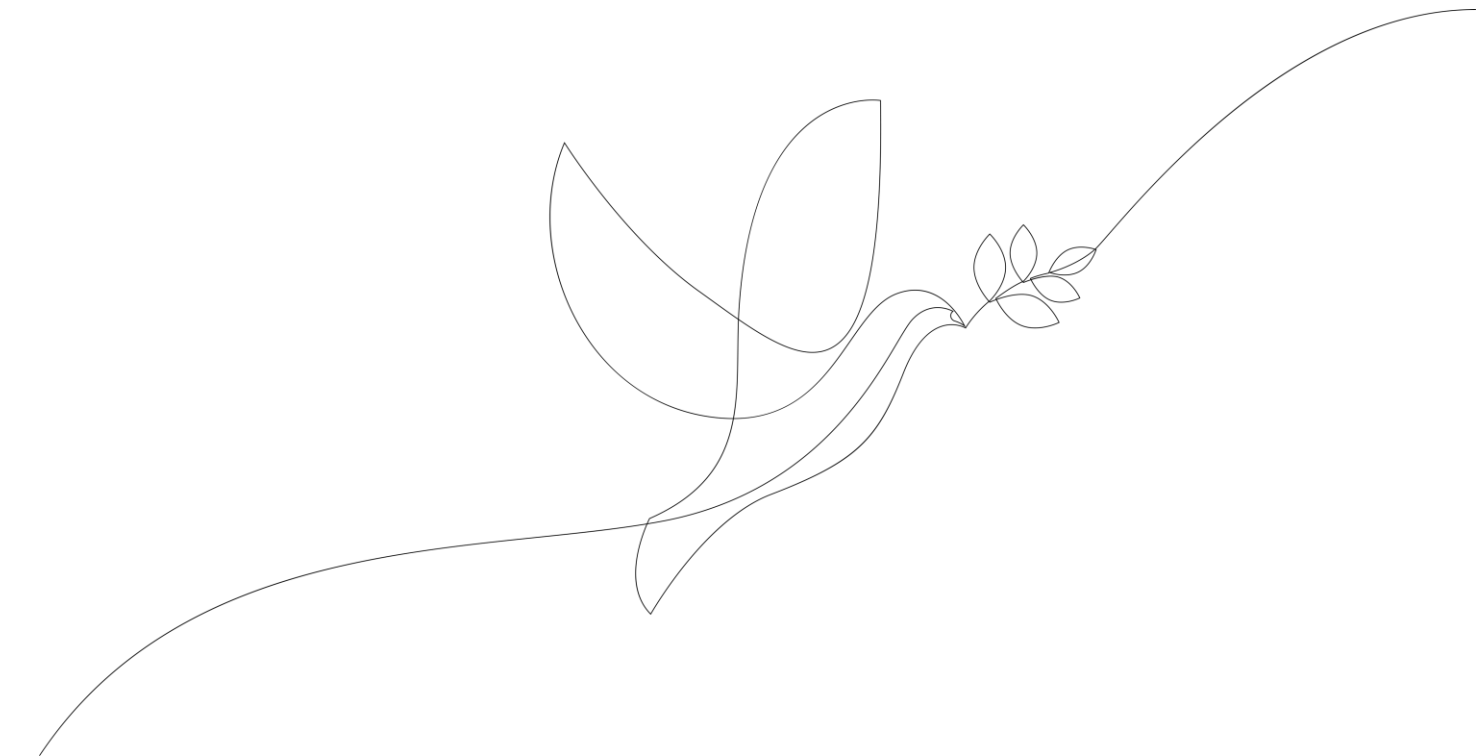
- Value can be held outside accounts or relationships.
- Value can be exchanged without account reconciliation.

(2) Allows clearing and settlement by **independent, private actors**.

- Leverages the existing institutional platform for payments.
- Decentralisation prevents tampering or unwanted changes to the rules.

(3) Protects consumers from profiling through **privacy by design**.

- Withdrawals and deposits are analogous to cash.
- Payers are anonymous and recipients are not.



The system must be private by design for consumers

Risk of **profiling** is **NOT** about knowing who the users of money are.

- OK to require **AML/KYC** for **recipients** of CBDC (for example, accountholders who withdraw tokens or merchants who accept them).
- OK to disallow **peer-to-peer** transactions.

Risk of **profiling** is about knowing how consumers spend their money .

- The identity of the sender **MUST NOT** be linked to:
 - the **recipient**
 - the **size**
 - **metadata** such as time, location, service providers, and so on.
- Payments by the same sender **MUST NOT** be linked to **each other**, implying that users **MUST NOT** be required to use wallet providers or registered wallets.

Privacy-enhancing technologies (**PETs**) can mitigate profiling risks.

- **Blind signatures** (viz. Chaum) and **privacy by design** are sufficient.



The system must enforce strong compliance rules

Vendors MUST be **authorised** by the system

Banks can perform verification in addition to AML/KYC checks

Consumers must have a way to **verify** that a vendor is authorised

Consumers MUST embed the identity of vendors (e.g. bank account information) into the transaction.

The system SHOULD require that tokens are provided **directly** to bank accounts of authorised vendors

The system MAY allow vendors to transfer tokens to other vendors, forming a chain.

Conditions for proper transfer can be enforced by banks **in the transfer channel** or at the time of **redemption**.



A new digital currency architecture: our approach

Three components:

Blind signatures, for privacy by design, with verifiable anonymity

- Similar privacy model to Chaum, Grothoff, Möser.
- Similar privacy model to BIS Swiss Centre “Project Tourbillon”.

Distributed ledgers, for immutability and institutional trust

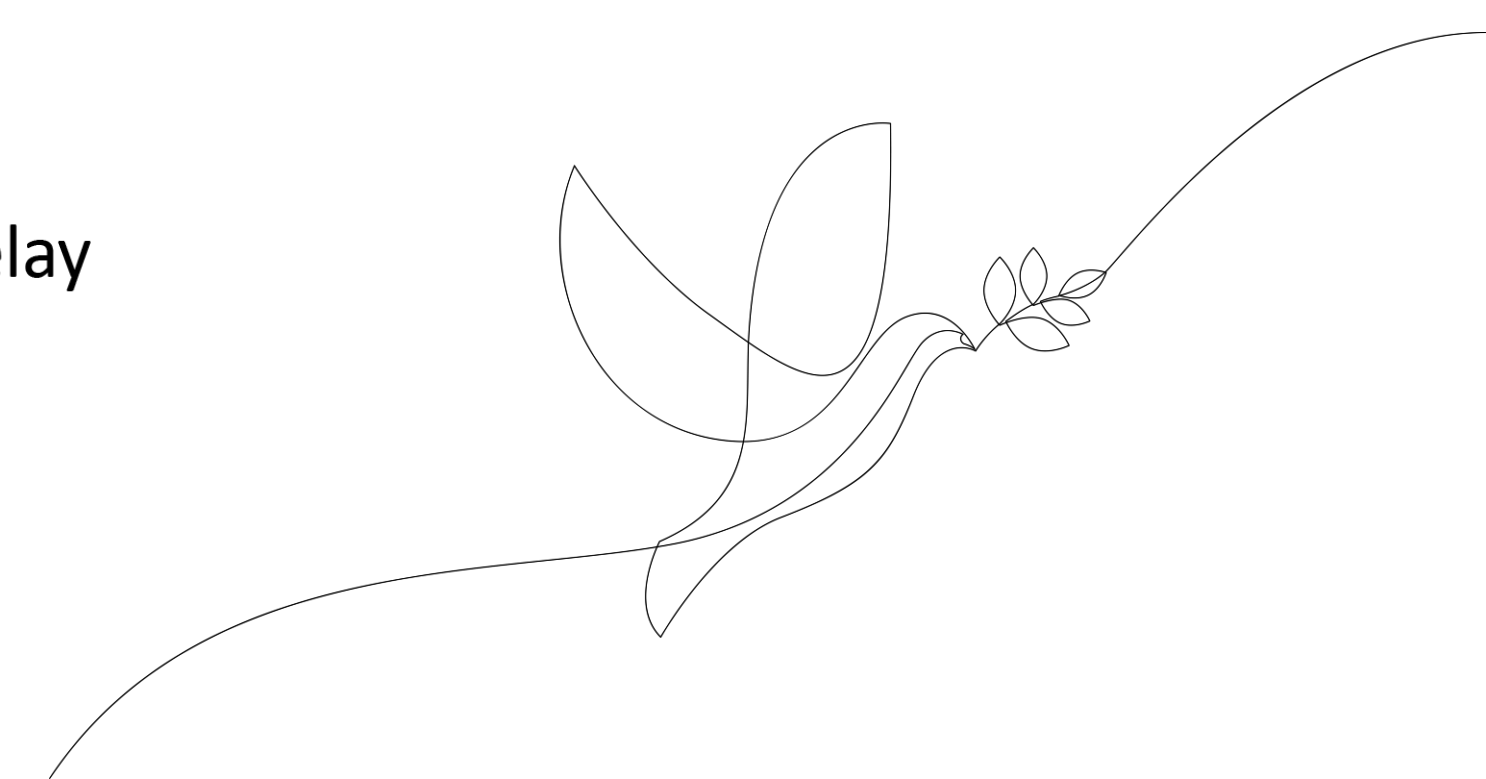
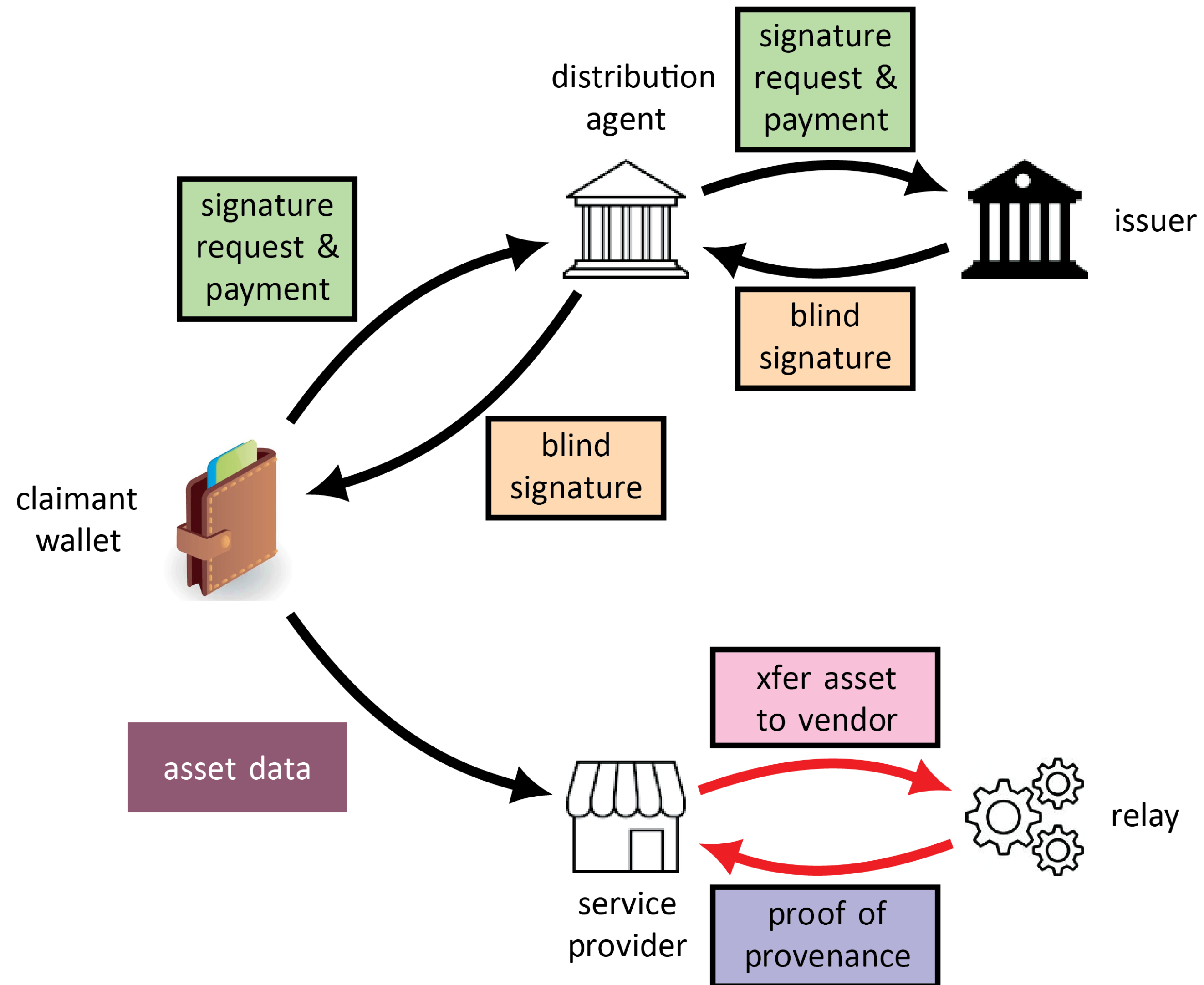
- Nodes are operated by independent service providers
- Assets are stored in non-custodial wallets

Unforgeable, stateful, oblivious (USO) assets, for scalability

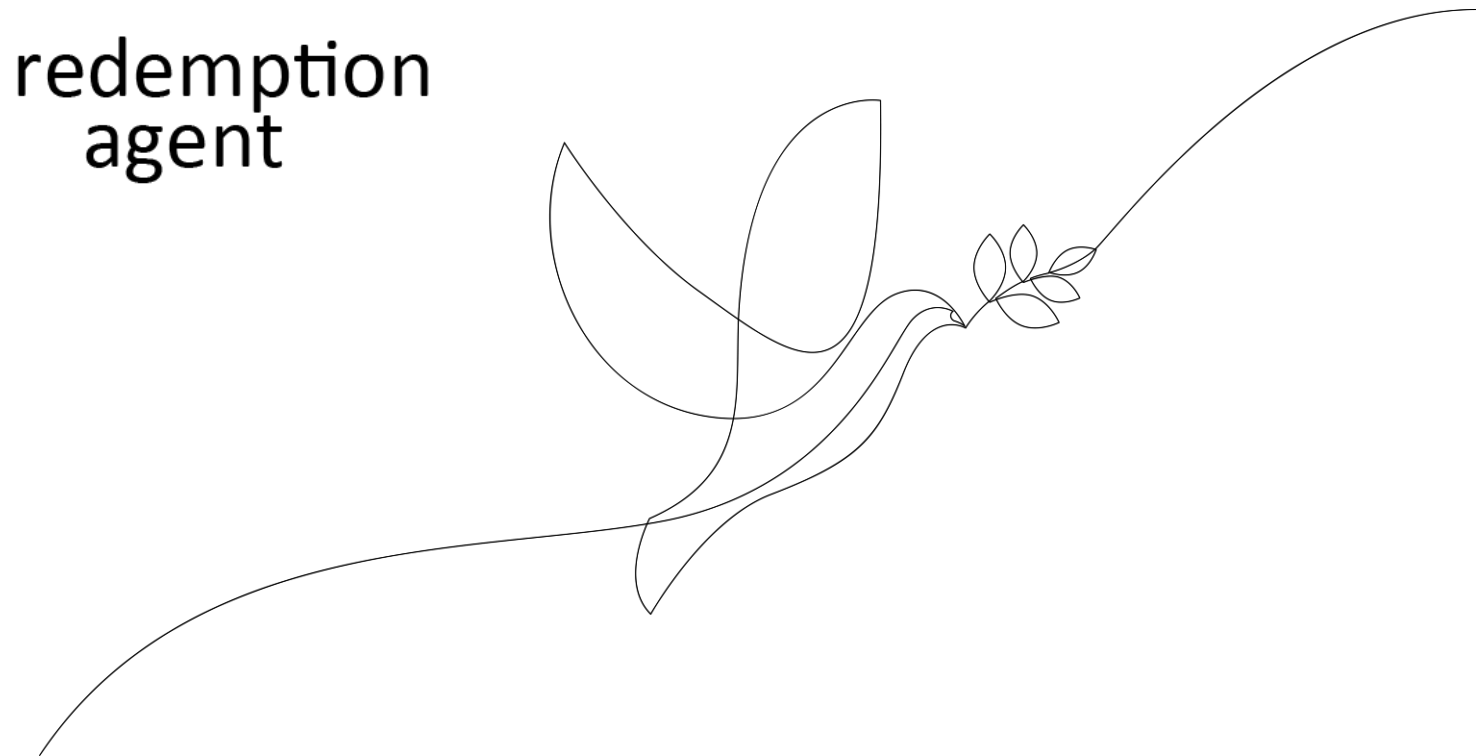
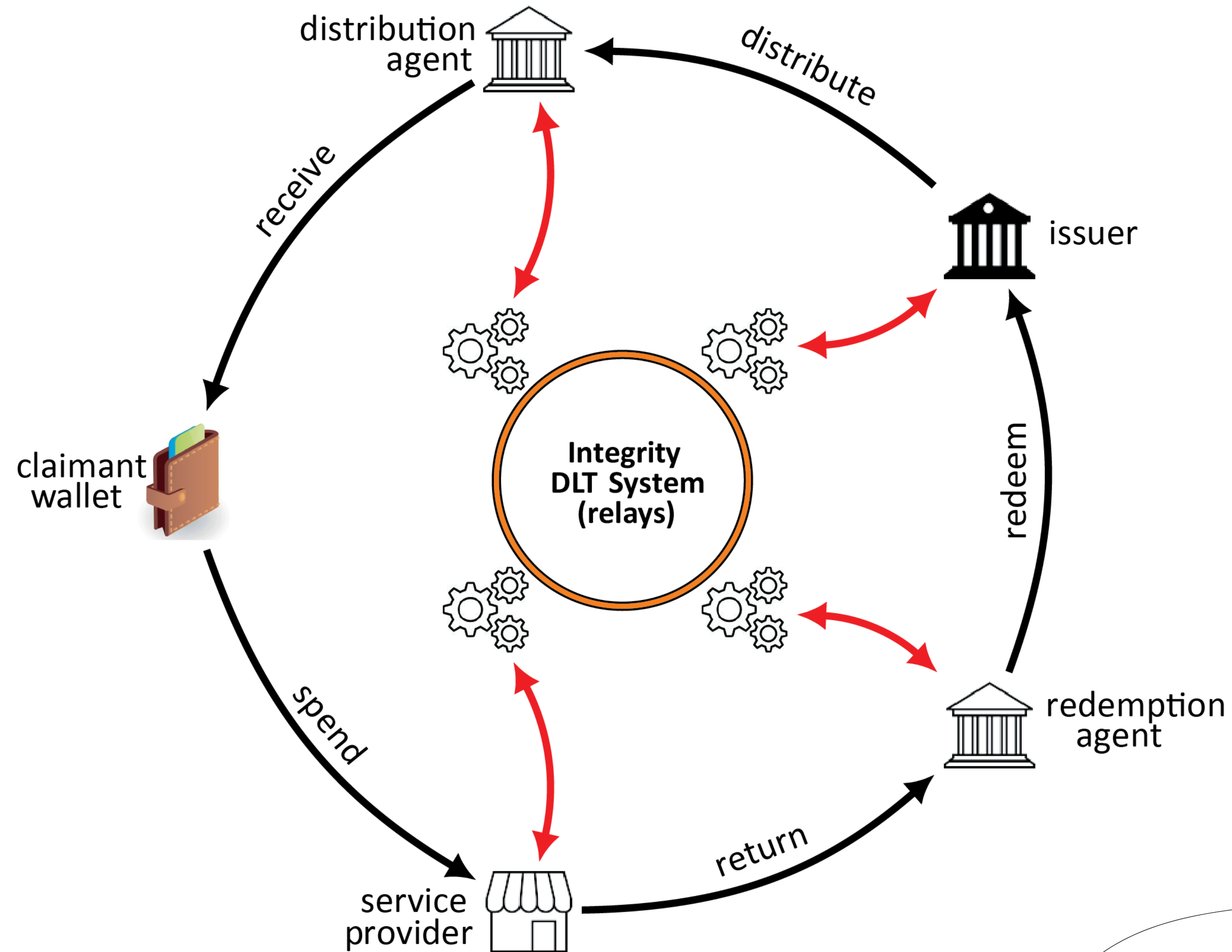
- Issuer does not maintain a database of assets (contrast with UTXO approaches)
- Issuer has no role in the “hot loop” of transactions



Digital payment claimant journey



Digital Payment life cycle





Thank you!

The Peace Coalition

Vancouver-Toronto-Montreal-Washington-London-Amsterdam-Basel-Geneva-Stockholm-Krakov-Kyiv