

Lessons Learned Under Pressure

Empathy-Driven Engineering for Privacy and Human Rights

Big Problems Often Feel Overwhelming

- When faced with complex social issues in any facet of life, it's easy to feel overwhelmed.
- Meaningful change begins with **active listening** and **collaborative building** of human-centered solutions.

Technology is not Magic

- Technology alone cannot save us. It must be wielded with **empathy**, **intention**, and **insight** from affected communities.
- Effective solutions require **active listening** and **collaboration**.

Real Lives, Real Risks

- Privacy is fundamental to **human safety** and **dignity**.
- **Privacy is for everyone.** Today's harmless information can become tomorrow's liability.
- **At-risk groups** face constant risk from digital surveillance.

"They took my phone... They beat me ... until I signed papers that said I was 'practicing debauchery'."

– Yasser, LGBTQ+ individual in Egypt, *Human Rights Watch*, 2020

"It is horrifying to me that they knew everything I was doing, who I was speaking with, my private thoughts at any moment they desired."

– Carine Kanimba, *Statement to US House Permanent Select Committee on Intelligence*, 2022

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

– Edward Snowden, whistleblower

Looking Back in Time

Case Studies From My Work

Arrests of Hong Kong Protesters Due to Telegram Group Membership

- While Telegram promised protection of group users by hiding their phone number, it was possible for authorities to “map” the entire address space by looking up all +852 numbers.
- Secure group communication was desperately needed to organize against Chinese government and avoid police interception.

Implemented Solution:

- Allowed Signal users to “opt-out” of phone number lookup.
- Improved contact discovery using secure enclaves (TEEs) to enforce rate limits and attest to behavior.
- Enabled username based addressing for true pseudonymous communications for those who need them.

Impact: Eliminated possibility for mass social graph reconstruction, allowing protesting with reduced fear of arrest. Signal is now #1 messaging app in HK.

COVID-19

- High rates of hospitalization, combined with quarantine protocols, resulted in extreme patient isolation from family and friends.
- Stay at home orders similarly resulted in elevated senses of isolation.
- Limited options available for secure video calls (necessary for HIPAA compliance).
- No user-friendly options for secure group calls.

Implemented Solution:

- Allocated thousands of “reserved” phone number blocks (+1-555) numbers for hospital patients to enable per room tablet setup for HIPAA compliant calling.
- Rapidly implemented end-to-end encrypted group calls using open-source technology, rolling out a public beta in mid-2020.

Impact: Enabled patients to connect with their doctors, loved ones, and friends and everyone to connect safely from home.

Black Lives Matters Protestors Arrested due to Facial Recognition

- BLM groups faced heightened surveillance during protests.
- Facial recognition, combined with mask bans, leading to mass arrests of attendees.
- ML-based facial recognition would regularly misidentify People of Color, leading to false arrests.
- **Additional Problem Identified:** Medics on the ground struggling to use existing tools to coordinate.

Implemented Solution:

- Use the same ML tools law enforcement was leveraging to anonymize and blur faces in protest photographs automatically.
- Coordinate with community leaders to distribute educational materials.
- Improved performance of Signal on low-bandwidth networks.

Impact: Reduced risk of identification/arrest. Allowed medics to communicate.

Internet Blackouts in Iran in Response to Women's Rights Protests

- Priority was on restoring secure communications, to enable activists to organize.
- Iran used Deep Packet Inspection (DPI), targeting TLS SNI headers.
- Domain Fronting was not viable due to large CDNs being down (Google, Amazon, Fastly).

Implemented Solution:

- Quickly deployed encrypted proxy servers hiding the **CONNECT** request from DPI.
- Launched the #IRanASignalProxy campaign, crowdsourcing proxy server hosting to evade IP-based blocking.

Impact: Enabled millions of daily secure connections, restoring activists' ability to organize safely in real time. Similar protections later rolled out worldwide as Encrypted Client Hello (ECH).

Amplified Oppression of Women Post Taliban Resurgence in Afghanistan

- Women urgently needed secure channels to safely coordinate evacuation efforts without Taliban detection.
- Taliban regularly checked phones for banned apps or signs of planned escape; secure apps needed to remain hidden or disguised.
- Afghan women required clear guidance on safely using digital tools to facilitate safe exits and secure refuge abroad.

Implemented Solution:

- Developed educational materials in local languages, specifically detailing secure communication techniques and evacuation procedures.
- Taught techniques for hiding apps, erasing traces, and securing devices from searches.

Impact: Directly enabled successful, safe evacuations.

Heightened Need for Advanced Encryption Tools Post-Dobbs

- Increased surveillance targeting reproductive healthcare communications; even period-tracking apps now need end-to-end encryption.
- Existing encryption methods (complex cryptography, key management) inaccessible to average users and developers.
- Centralized trust – even through non-profits like Signal – considered too risky for vulnerable women and medical practitioners.

Implemented Solution:

- Open-sourced novel distributed key management protocol that changes the **trust model**, allowing users to interact with confidence.
- Utilizing distributed cryptography and hardware security, to enable secure back and recovery of keys with **simple PIN authentication**.

Impact: Valuable research endeavor that released a new protocol in 2024. May be managed by Cloudflare going forward.

Moving Forward

Applying What We've Learned

How to Connect

- Local NGOs, advocacy organizations, human rights groups
- Universities, legal aid clinics, refugee support orgs
- Human rights/social justice events and workshops
- Collaborations with domain-experts (activists, affected)

Connect with Respect

- Humility and active listening first
- Design solutions **together** in community, not in isolation
- Clearly communicate your intent and build trust slowly
- Ensure confidentiality and informed consent at every step
- Maintain transparency and accountability throughout

Privacy is a Human Right

“Everyone has the right to be protected from arbitrary interference with their privacy”

– UN Universal Declaration of Human Rights, Article 12

- Privacy is essential to **autonomy**, **dignity**, and **freedom**—especially critical on social media, where data becomes identity.

Your Role in Protecting Privacy

- What small steps can you take today to help protect privacy – either your own or someone else's?
- How can engineers, policymakers, and everyday users work together to build a future where privacy is a right, not a privilege?
- If privacy is a human right, what responsibility do you have to defend it?

Taking Action Under Pressure

- Big problems often feel overwhelming, but meaningful change **starts** with small, decisive actions.
- Every crisis has needs that can be identified through **collaboration** – the greatest innovations in privacy and human rights have emerged under pressure.
- We don't need perfect solutions, we need progress – even imperfect tools can save lives when built with **empathy**.

“The secret is to begin.”

– Moxie Marlinspike, creator of Signal