Defending Messaging Apps Against Spyware Using Data Diodes

Peter Story
Clark University
Worcester, Massachusetts, USA
PeStory@clarku.edu

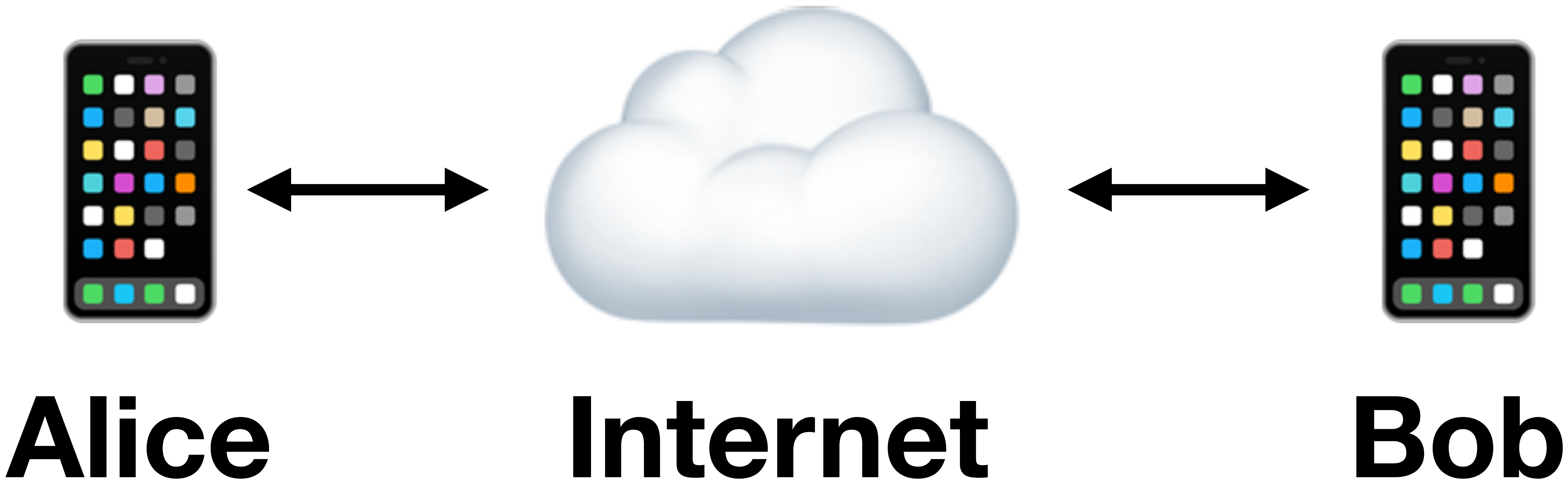
How Secure are Secure Messaging Apps?

Signal

WhatsApp

iMessage

End-to-end Encryption (E2EE)



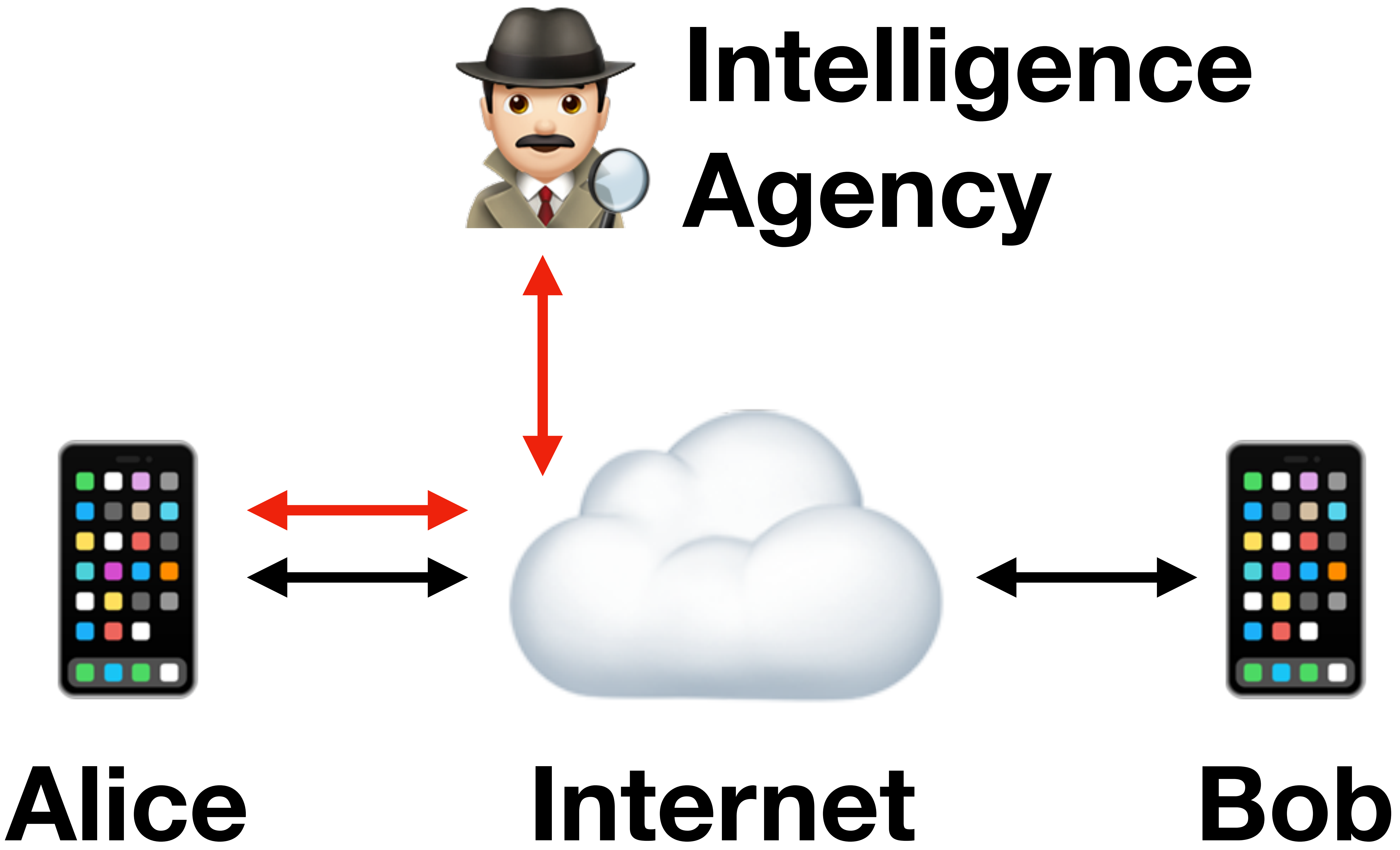
Alice

Internet

Bob

E2EE defends against passive government surveillance

Spyware

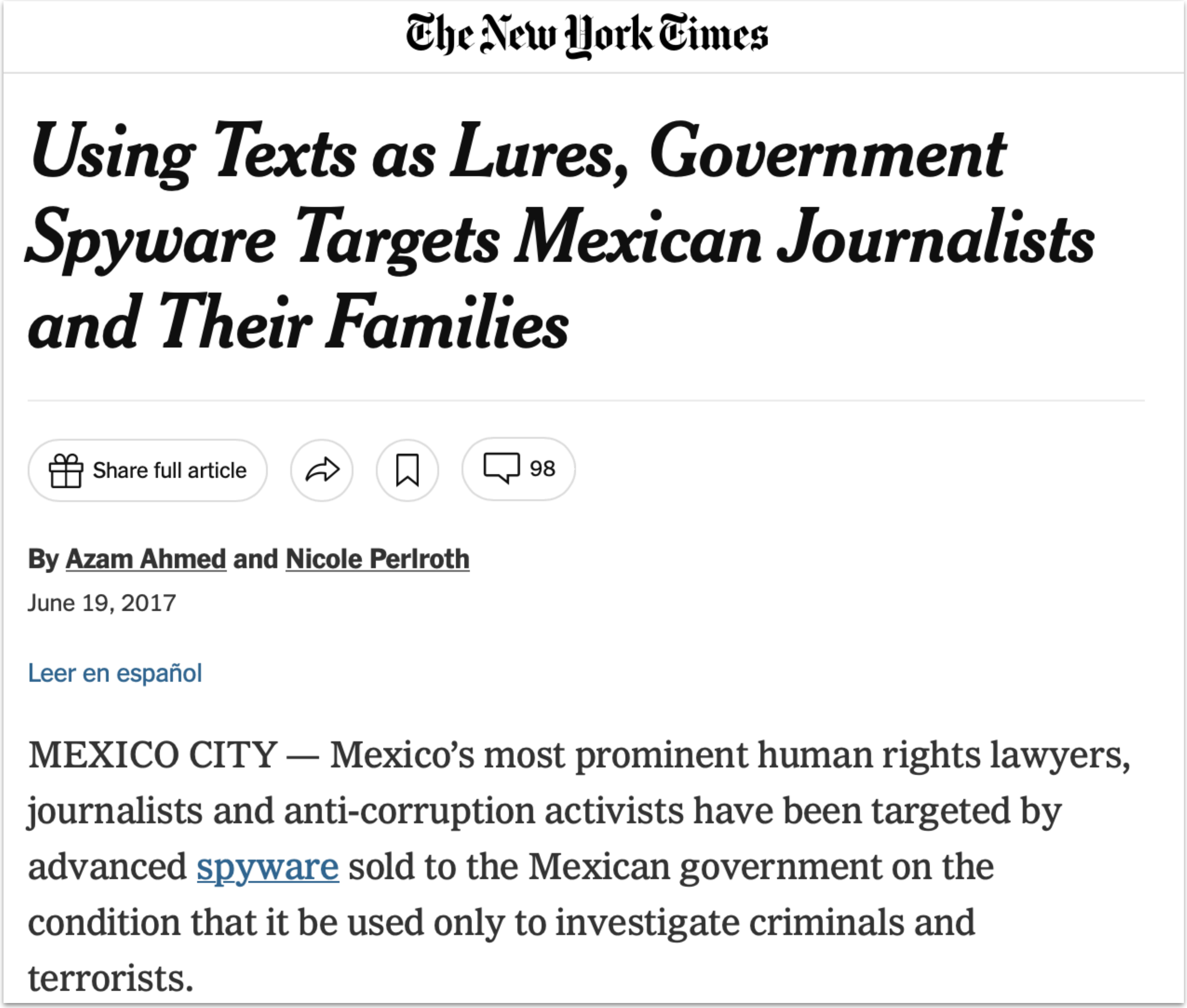


Intelligence Agency

Alice

Internet

Bob



The New York Times

Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families

By Azam Ahmed and Nicole Perlroth

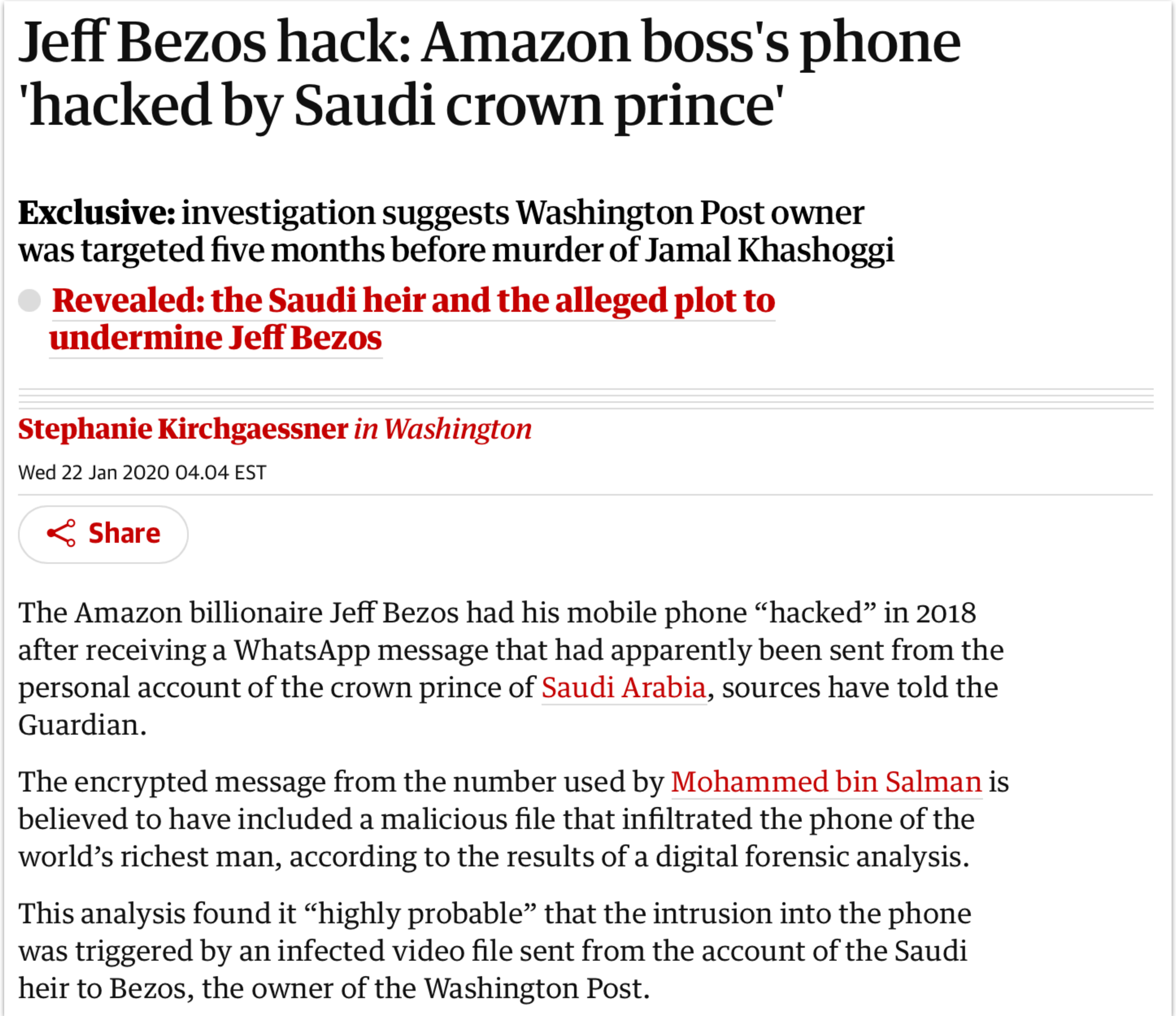
June 19, 2017

Leer en español

MEXICO CITY — Mexico's most prominent human rights lawyers, journalists and anti-corruption activists have been targeted by advanced spyware sold to the Mexican government on the condition that it be used only to investigate criminals and terrorists.

Carmen Aristegui

The Guardian



Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

Exclusive: investigation suggests Washington Post owner was targeted five months before murder of Jamal Khashoggi

- **Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos**

Stephanie Kirchgaessner *in Washington*

Wed 22 Jan 2020 04.04 EST

The Amazon billionaire Jeff Bezos had his mobile phone “hacked” in 2018 after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, sources have told the Guardian.

The encrypted message from the number used by Mohammed bin Salman is believed to have included a malicious file that infiltrated the phone of the world’s richest man, according to the results of a digital forensic analysis.

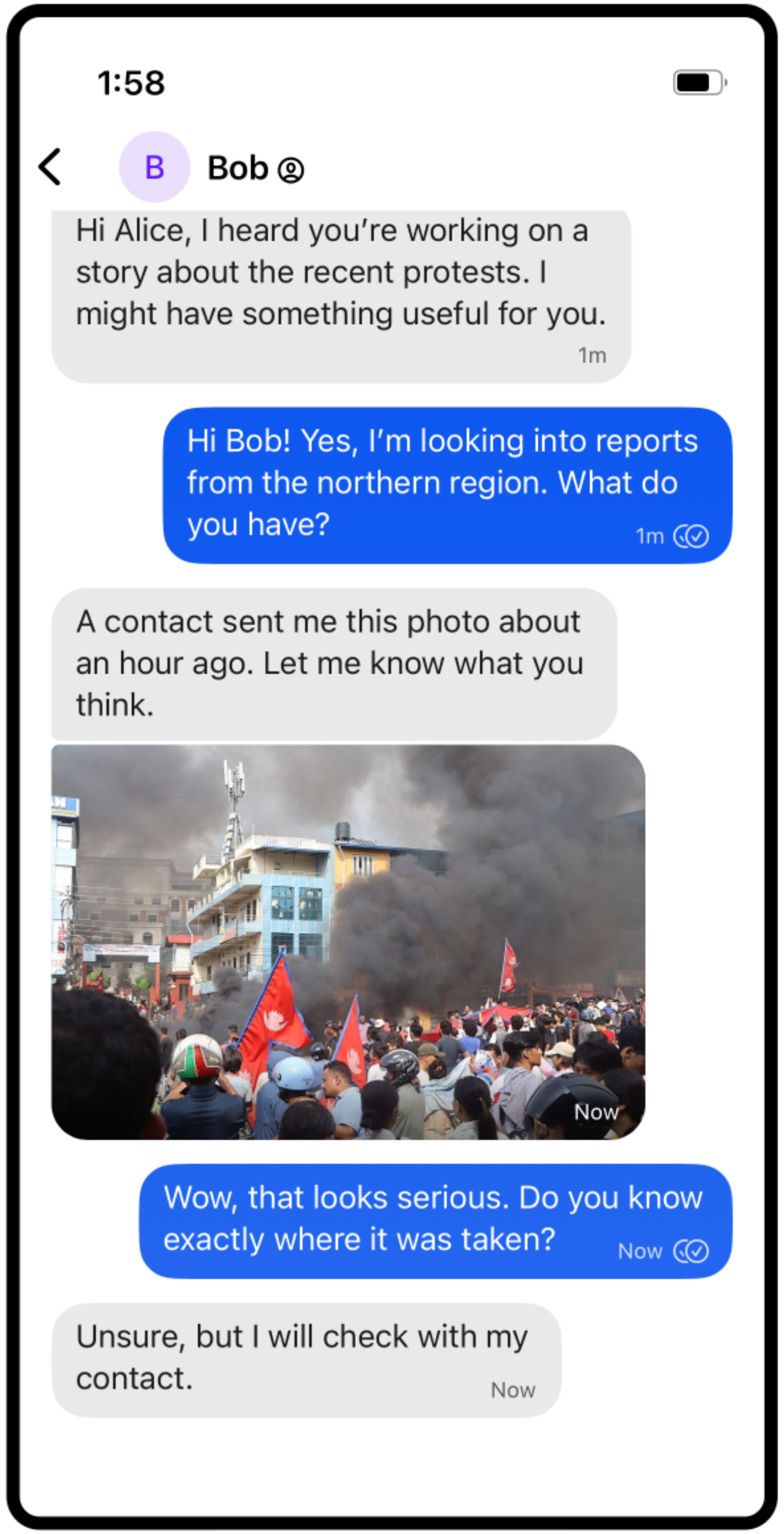
This analysis found it “highly probable” that the intrusion into the phone was triggered by an infected video file sent from the account of the Saudi heir to Bezos, the owner of the Washington Post.

Jeff Bezos

Jamal Khashoggi

Secure Messaging Apps

- E2EE defends against passive government surveillance...
    - ...but offers no protection against spyware
- How to defend against spyware?



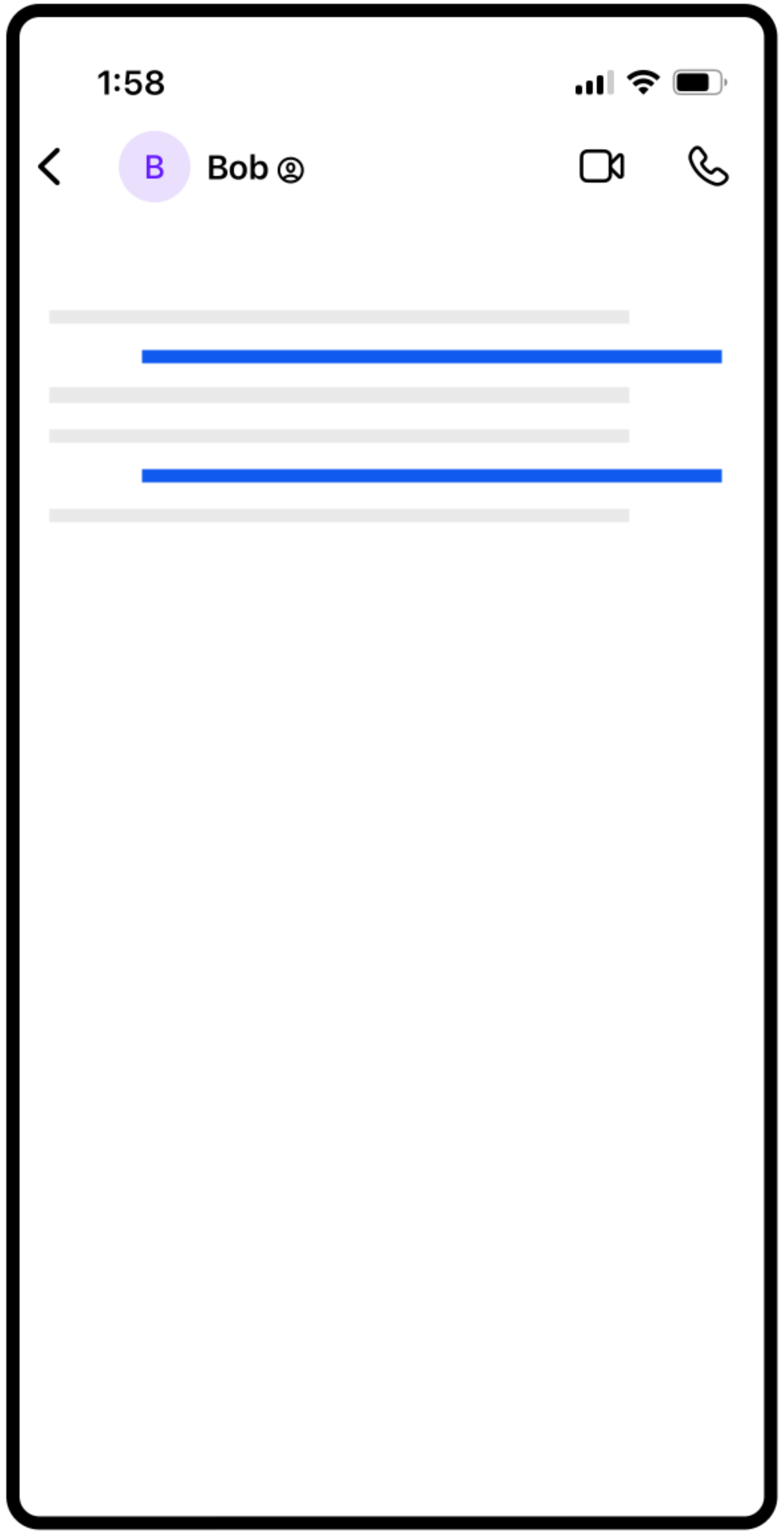
Hi Alice, I heard you’re working on a story about the recent protests. I might have something useful for you. 1m

Hi Bob! Yes, I’m looking into reports from the northern region. What do you have? 1m

A contact sent me this photo about an hour ago. Let me know what you think.

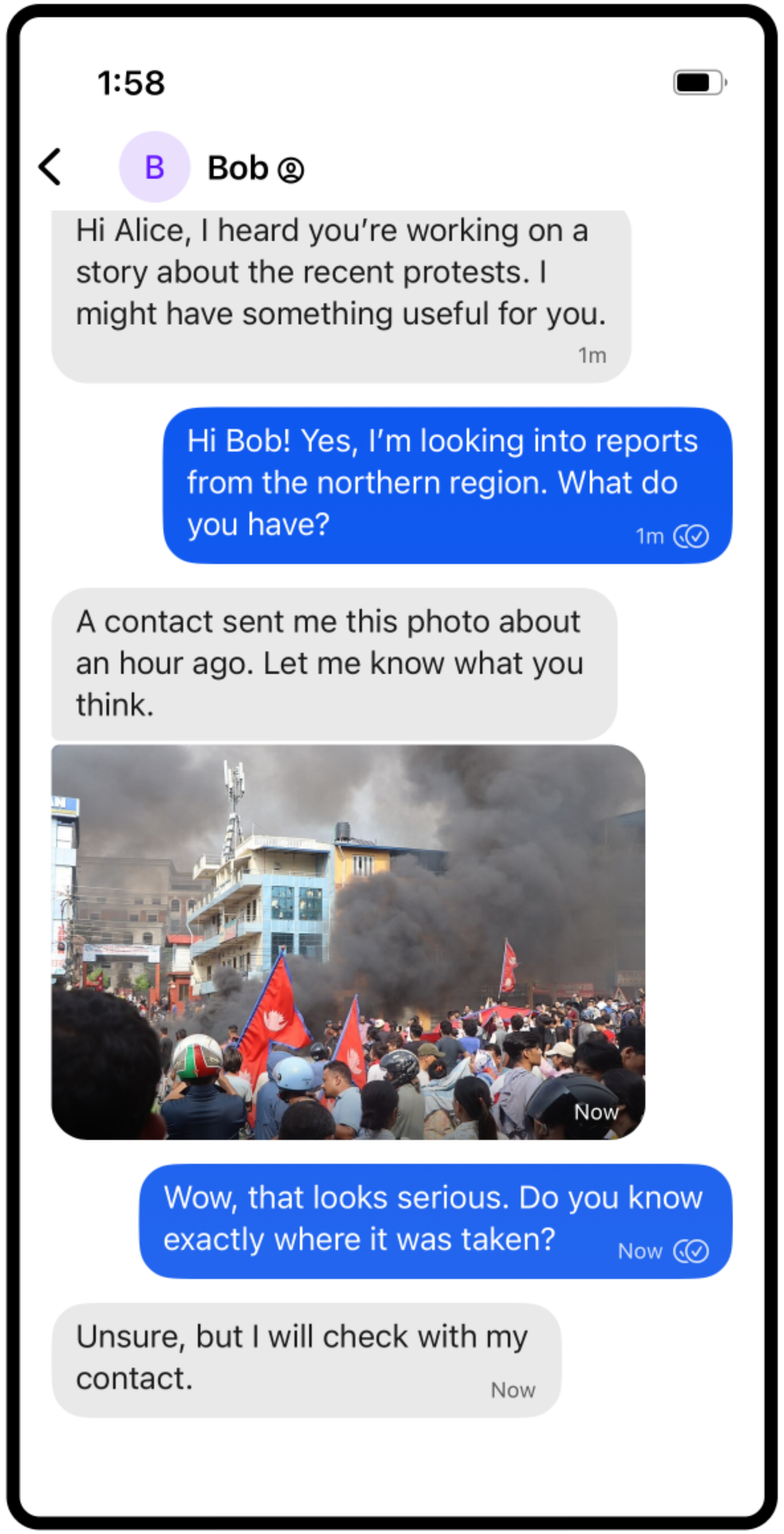
Wow, that looks serious. Do you know exactly where it was taken? Now

Unsure, but I will check with my contact. Now



Internet-connected

One-way



Hi Alice, I heard you're working on a story about the recent protests. I might have something useful for you. 1m

Hi Bob! Yes, I'm looking into reports from the northern region. What do you have? 1m

A contact sent me this photo about an hour ago. Let me know what you think.

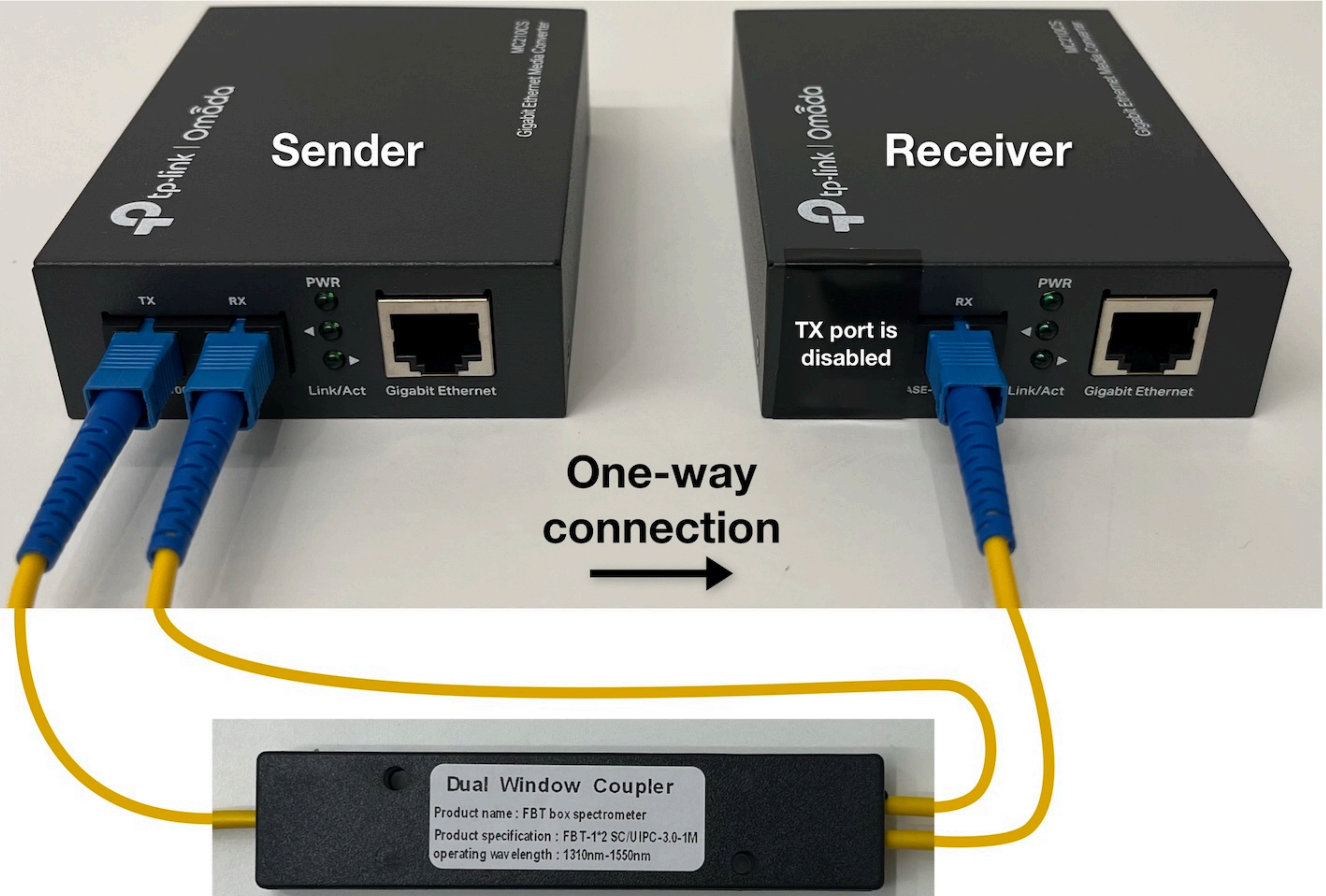
Now

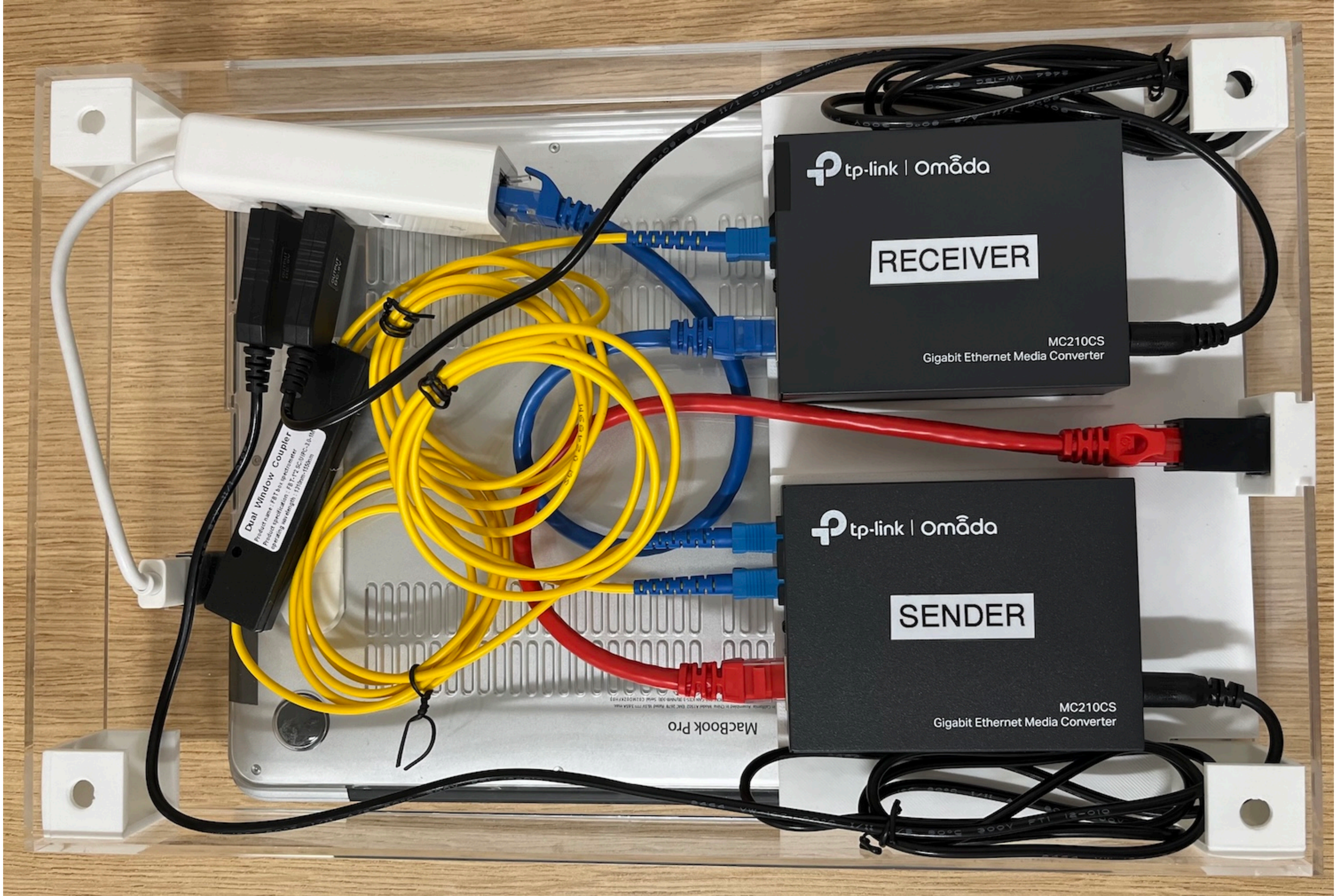
Wow, that looks serious. Do you know exactly where it was taken? Now

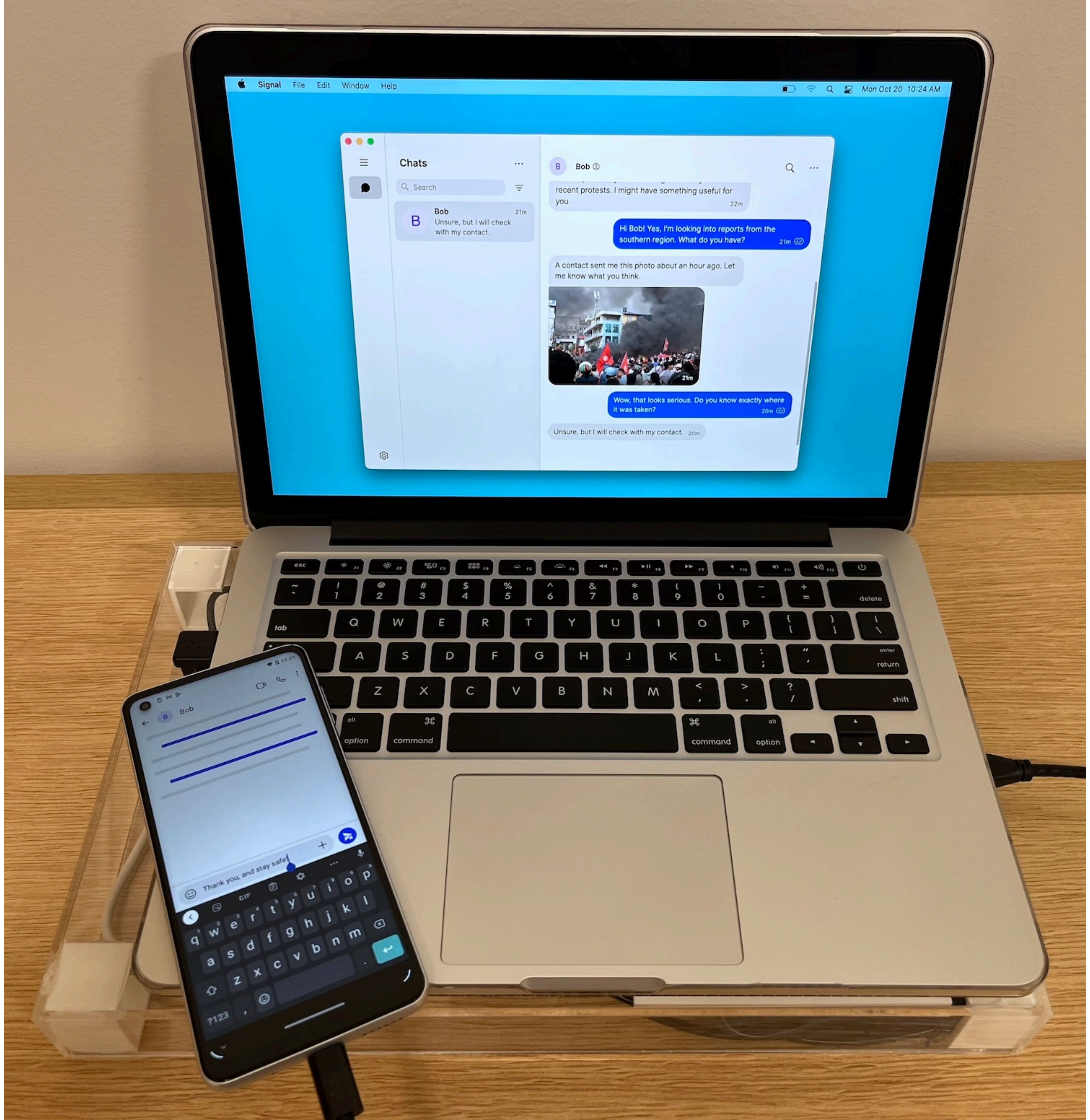
Unsure, but I will check with my contact. Now

Air-gapped

Data Diode


Sender
Receiver
TX port is disabled
One-way connection
tp-link | Omada
MC210CS
Gigabit Ethernet Media Converter
TX
RX
PWR
Link/Act
Gigabit Ethernet
Dual Window Coupler
Product name : FBT box spectrometer
Product specification : FBT-1*2 SC/UIPC-3.0-1M
operating wavelength : 1310nm-1550nm


tp-link | Omada
RECEIVER
MC210CS
Gigabit Ethernet Media Converter
tp-link | Omada
SENDER
MC210CS
Gigabit Ethernet Media Converter
Dual Window Coupler
Product name : FBT box spectrometer
Product specification : FBT-1*2 SC/UPC-3.0-1M
operating wavelength : 1310nm-1550nm
MacBook Pro



recent protests. I might have something useful for you. 22m

Hi Bob! Yes, I'm looking into reports from the southern region. What do you have? 21m

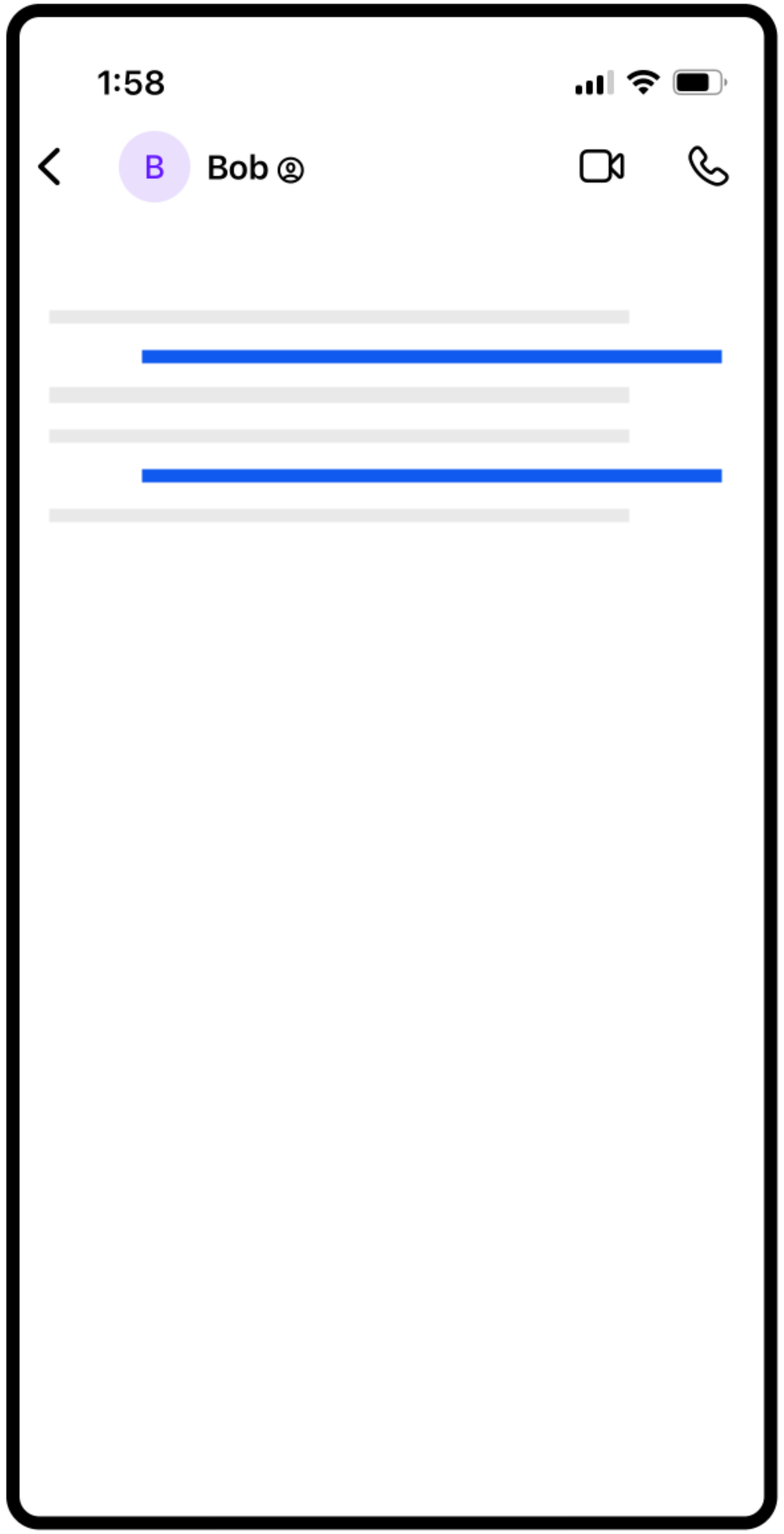
A contact sent me this photo about an hour ago. Let me know what you think.

21m

Wow, that looks serious. Do you know exactly where it was taken? 20m

Unsure, but I will check with my contact. 20m

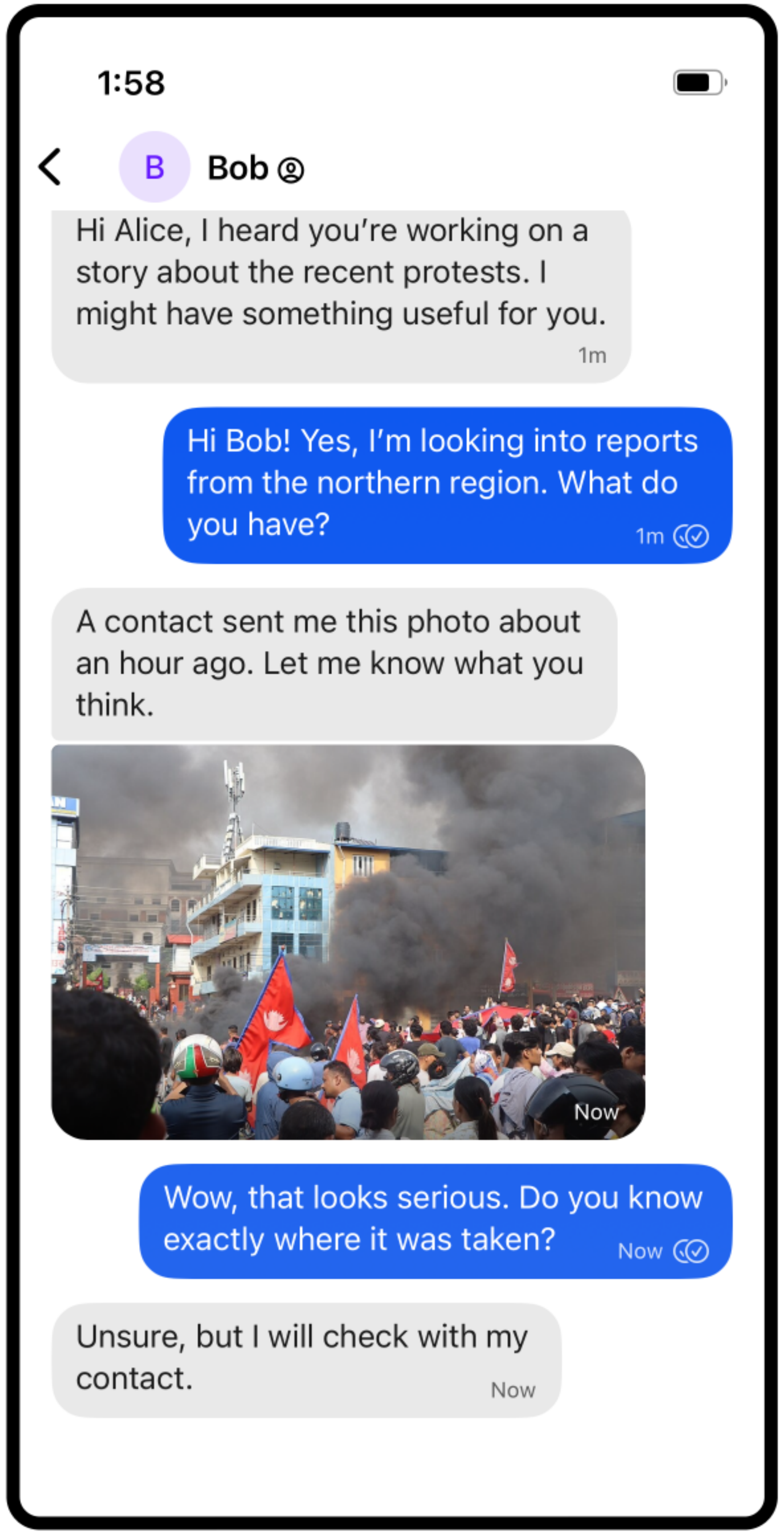
Alice’s Devices



Internet-connected

One-way

pydiode



Hi Alice, I heard you’re working on a story about the recent protests. I might have something useful for you. 1m

Hi Bob! Yes, I’m looking into reports from the northern region. What do you have? 1m

A contact sent me this photo about an hour ago. Let me know what you think.

Now

Wow, that looks serious. Do you know exactly where it was taken? Now

Unsure, but I will check with my contact. Now

Air-gapped

Spyware Defense Protocol

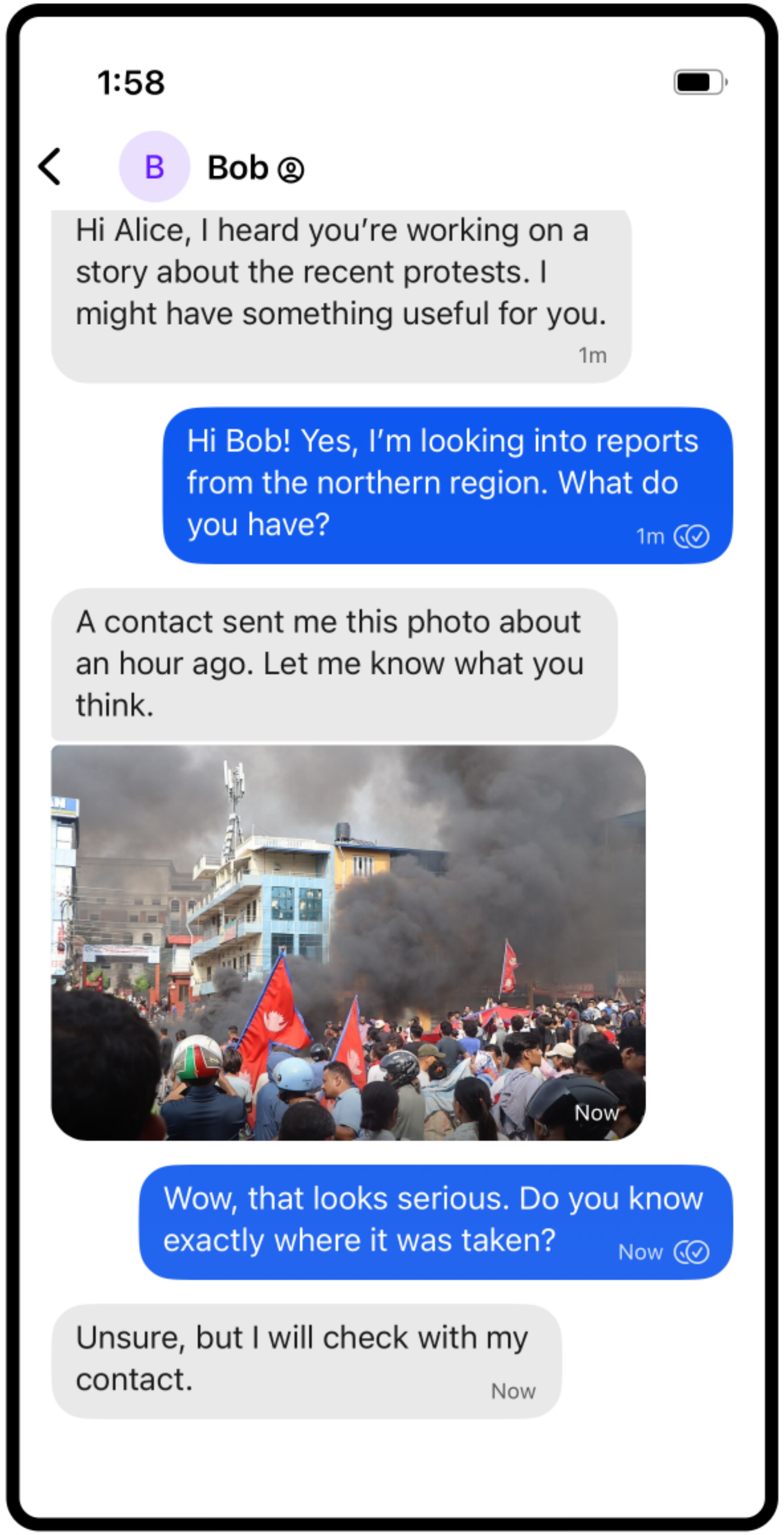
- Initial setup
- Incoming messages
- Outgoing messages

Initial Setup

- On her air-gapped device, Alice:
  - Generates a public private key pair
  - Displays the public key as a QR code
- On her internet-connected device, Alice:
  - Enables the Spyware Defense feature
  - Scans the public key’s QR code to register it server-side

Incoming Messages

- Bob composes a message for Alice
  - Prior to the standard Signal Protocol, Bob's client encrypts the message with Alice's Spyware Defense Public key
- Alice receives the incoming message on her internet-connected device
- Alice's client sends the message to her air-gapped device, which automatically decrypts and displays it



Hi Alice, I heard you're working on a story about the recent protests. I might have something useful for you. 1m

Hi Bob! Yes, I'm looking into reports from the northern region. What do you have? 1m

A contact sent me this photo about an hour ago. Let me know what you think.

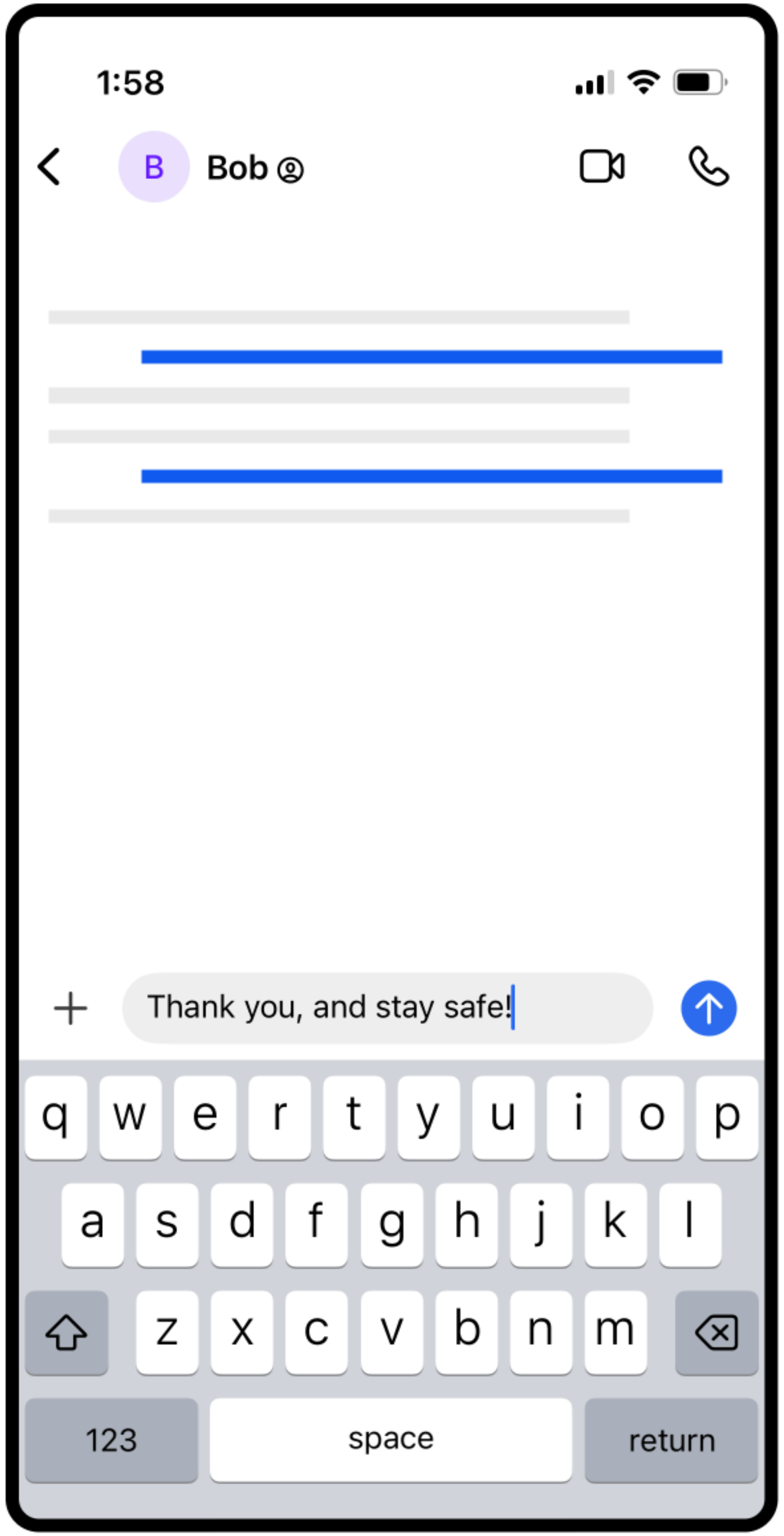
Now

Wow, that looks serious. Do you know exactly where it was taken? Now

Unsure, but I will check with my contact. Now

Outgoing Messages

- Alice composes a message for Bob on her internet-connected device
    - If Bob has enabled the Spyware Defense feature, Alice's client encrypts the message with Bob's Spyware Defense Public key
    - Alice's client encrypts the message with her Spyware Defense Public key before storing it at rest
- When next connected to the air-gapped device, Alice's client sends the message for display in the conversation thread



Spyware Defense Protocol

- The underlying messaging app’s protocol is not changed: message payloads simply have another layer of encryption
- Because a user’s Spyware Defense private key is only stored on their air-gapped device:
  - Message confidentiality is protected
  - The attack surface of the internet-connected device is smaller

Threat Model

- What if Alice’s internet-connected device is compromised?
  - Alice’s received messages are unreadable
  - Attacker could see who Alice is communicating with
  - Alice’s outgoing messages could be read as they are composed
  - Attacker could register their own Spyware Defense key pair

Threat Model

- What if **Bob's** internet-connected device is compromised?
- If Bob is using the spyware defense feature:
  - **Bob's** received messages are unreadable
  - Attacker could see who **Bob** is communicating with
  - **Bob's** outgoing messages could be read as they are composed
  - Attacker could register their own Spyware Defense key pair

Threat Model

- What if **Bob’s** internet-connected device is compromised?
- If Bob **is not** using the spyware defense feature:
  - All of Bob’s sent and received messages are readable

Threat Model

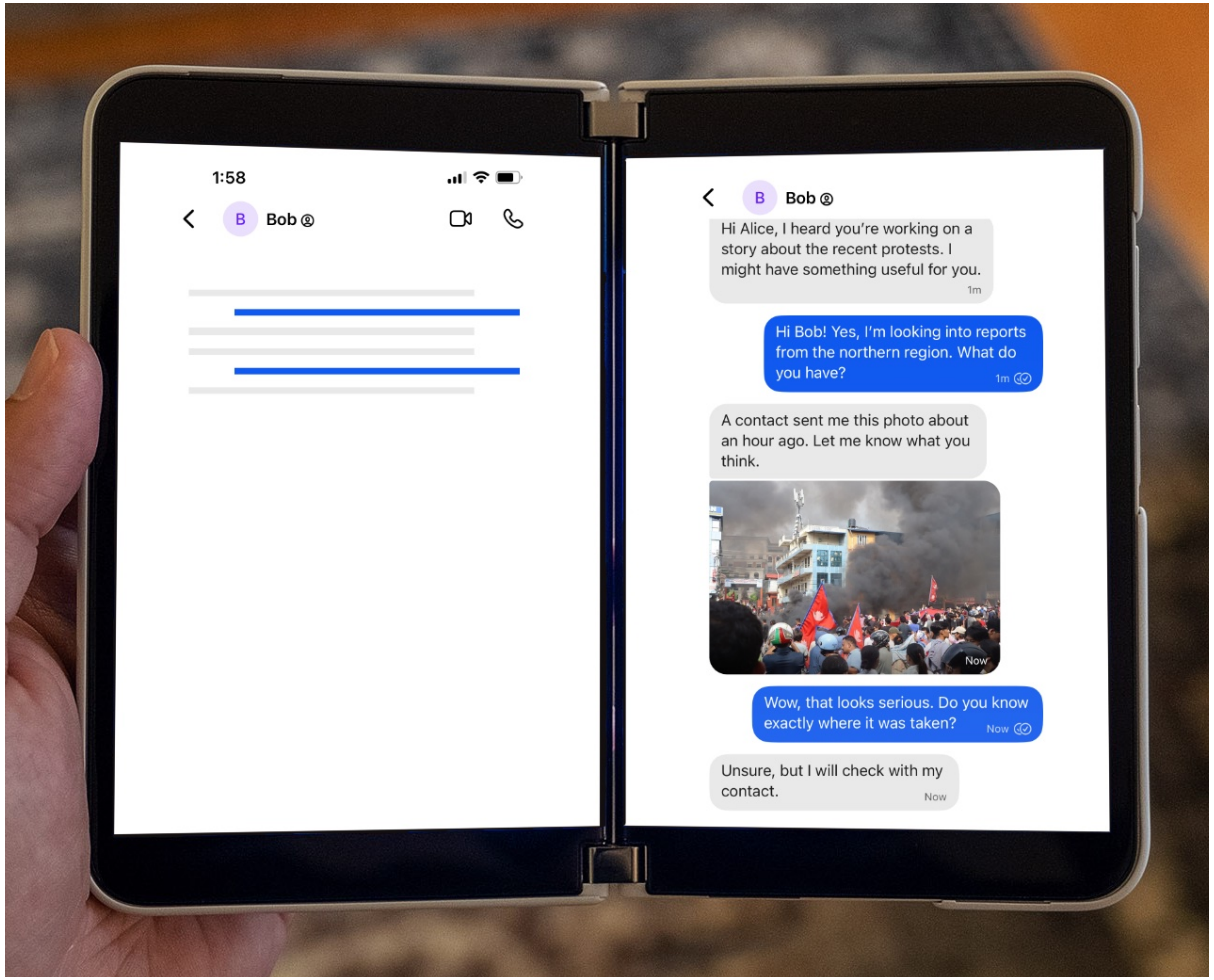
- What if **Alice’s air-gapped device** is compromised?
  - Alice’s messages cannot be exfiltrated through the network
  - Message history could be tampered with or deleted
  - Possible data exfiltration using side-channel attacks

Threat Model Summary

- If Alice and Bob enable the Spyware Defense feature:
  - Smaller attack surface and attack window
- If only Alice enables the Spyware Defense feature:
  - All messages could be accessed on Bob’s device

Obstacles to Adoption: Hardware

- The Spyware Defense feature requires additional hardware
- Today, the hardware is bulky
- In the future, the hardware could be miniaturized



Hi Alice, I heard you're working on a story about the recent protests. I might have something useful for you. 1m

Hi Bob! Yes, I'm looking into reports from the northern region. What do you have? 1m

A contact sent me this photo about an hour ago. Let me know what you think. Now

Wow, that looks serious. Do you know exactly where it was taken? Now

Unsure, but I will check with my contact. Now

Original Photo Credit: The Verge

Obstacles to Adoption: Software

- The messaging app must be modified to support Spyware Defense keys
- More limited protections could be implemented today in Signal
  - Alice’s client would encrypt incoming messages using her public key. This would:
    - Shrink the attack surface of Alice’s internet-connected device
    - Limit the attack window

Please get in touch!

Visit: https://datadiode.net/

Email me: PeStory@clarku.edu

CLARK
UNIVERSITY

CLARK UNIVERSITY
FIAT
LUX
MDCCCLXXXVII