



# Technological vs. Political Approaches to Surveillance

Nadim Kobeissi

PRISMBreak – New York City





TOP SECRET//SI//ORCON//NOFORN



Communication Board Mail



# USED MOST



# Given a problem,

Would you rather:

- Obtain a quick solution,
- or –
- Give up what you're doing  
and sit down to understand  
the problem?



## PRISM/US-984XN Overview

OR

## SIGAD Used **Most** in NSA Repo Overview



April 2013





# People today

“Let’s solve a global surveillance apparatus built thanks to strong shared realist foreign policy convictions doubled by domestic assurances...



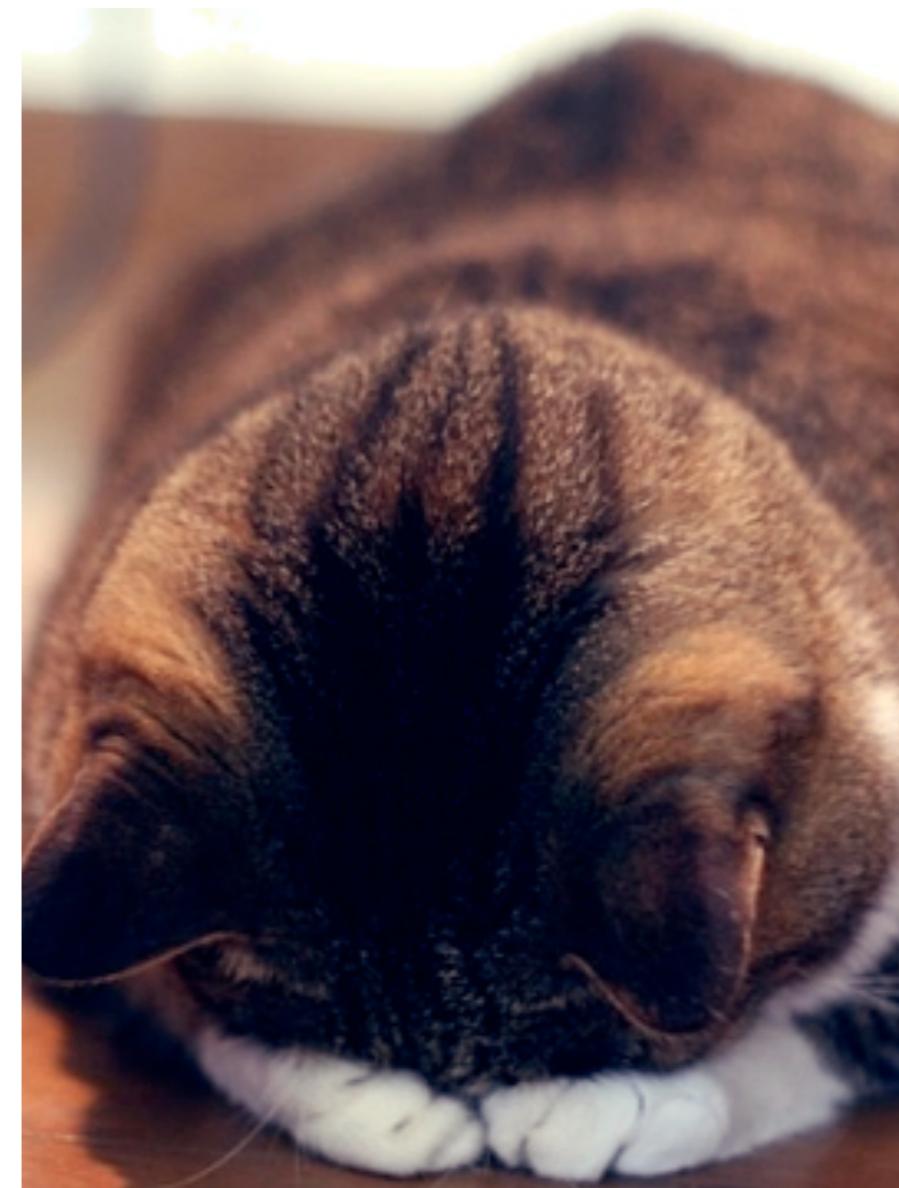
**WITH AN APP.”**



# People today

“No wait, I mean, that’s  
not the end of the line!

**WE’LL USE MULTIPLE  
APPS.”**





# Encryption tools

We can be optimistic about:

- Research.
- Availability.
- Variety.



The screenshot shows a Microsoft WordPad window titled "mein-key - WordPad". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Einfügen", "Format", and "?". The toolbar contains icons for file operations like Open, Save, Print, and Find. The main text area displays a PGP public key block. It starts with "-----BEGIN PGP PUBLIC KEY BLOCK-----", followed by "Version: GnuPG v1.4.3-cvs (MingW32)". The key itself is a long string of binary-like characters (0s and 1s). It ends with "-----END PGP PUBLIC KEY BLOCK-----". A status bar at the bottom says "Drücken Sie F1, um die Hilfe aufzurufen."

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3-cvs (MingW32)

mQGiBEPEO1ARBADP1bT8KfDJMjuOdLQrggk04zZb44sSEv
UnvQSngP2L4bzHjPsIV1WiWY1gers5vzPUkvCOb6SOx6QW
KgcAbMIwkAyVJbbxYPq/MbXavtANqbKZQ7MuFxn2WEZM3
w8czwZLTI1LKRvNTIF9Lg5kEAI+nzPfkUg7YUDXCAbJAIn
rDWqF2jDiaHZ102bGW1M5bmnnyApjIfssFdncrq4X/HqOR
3+oeny2xpiWSRarEP290OmXVLVqsSX+MAavaVBgfXJ4mgT
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33
D78kHwDuuJqKJh8+e4bUddEKdNVUOOmkZaHA/SfJmI9oku
g6iLAFc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGE
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2Vs2G9yZi5k2T6IYA
IwYLCQgHawIEFQIIAwQWAgnMBAh4BAheAAAoJECqKerJJXJ
QNc6vZmt4SGNPYkuAJ4ik20hE2iUr8wf53fyce+MbIkubb
8s1FOi7GfRAo41JLuZttg15cffKbNCBnXQJXREwnlhFtYb
5USzzcZRR3i3Ieikn2OXNdUsIFKg2Ywj21/2Cecq23Mn0e
vyFujFVQNm1Y4JFGRg0arWWOf7aSfR7rK+iTw8AAwUEAI
mnSGPgka/L6yWwrMn315SA8U+FqBohkgIzN8BCguqqcyse
8jzOR6QY7OXV5R/GcPE+O6U0RLRzJBadoyEmD/G29VhHyg
+bJPMgtB+JnmX2apIYbGFAQDiEkEGBECAAkFAkPE03ICGw
pACfUyuODaNmaLsOROGGCUE1mV+e8hAAmgK+xvYjsezXzJ
=J4dH
-----END PGP PUBLIC KEY BLOCK-----
```



# But what about...

- Accessibility?
- Instigating social debate?
- Forcing new laws to limit abuse?
- Resolving the dependence on surveillance to advance realist foreign policies?
- Socially solving an issue that is at root, social?

mein-key - WordPad

datei Bearbeiten Ansicht Einfügen Format ?

----BEGIN PGP PUBLIC KEY BLOCK----

Version: GnuPG v1.4.3-cvs (MingW32)

mQGiBEPEO1ARBADP1bT8KfDJMjuOdLQrggk04zZb44sSEv  
UnvQSngP2L4bzHjPsIV1WiWY1gers5vzPUkvCOb6SOx6QW  
KgcAbMIwkAyVJbbxYPq/MbXavtANqbKZQ7MuFxnxWEZM3  
w8czwZLTI1LKRvNTIF9Lg5kEAI+nzPfkUg7YUDXCAbJAIn  
rDWqF2jDiaHZ102bGW1M5bmnnyApjIfssFdncrq4X/HqOR  
3+oeny2xpiWSRarEP2900mXVLVqsSX+MAavaVBgfXJ4mgT  
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33  
D78kHwDuuJqKJh8+e4bUddEKdNVU00mkZaHA/SfJmI9oku  
g6iLAFc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGE  
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2Vs2G9yZi5k2T6IYA  
IwYLCQgHawIEFQIIAwQWAgnMBAh4BAheAAAoJECqKerJJXJ  
QNc6vZmt4SGNPYkuAJ4ik20hE2iUr8wf53fycE+MbIkubb  
8s1FOi7GfRAo41JLuZttg15cffKbNCBnXQJXREwnlhFtYb  
5USzzcZRR3i3Ieikn2OXNdUsIFKg2Ywj21/2Cecq23Mn0e  
vyFujFVQNm1Y4JFGRg0arWWOf7aSfR7rK+iTw8AAwUEAI  
mnSGPgka/L6yWwrMn315SA8U+FqBohkgIzN8BCguqgcyse  
8jz0R6QY7OXV5R/GcPE+O6U0RLRzJBadoyEmD/G29VhHyg  
+bJPMgtB+JnmX2apIYbGFAQDiEkEGBECAAkFAkPE03ICGw  
pACfUyuODaNmaLsOROGGCUE1mV+e8hAAmgK+xvYjsezXzJ  
=J4dH

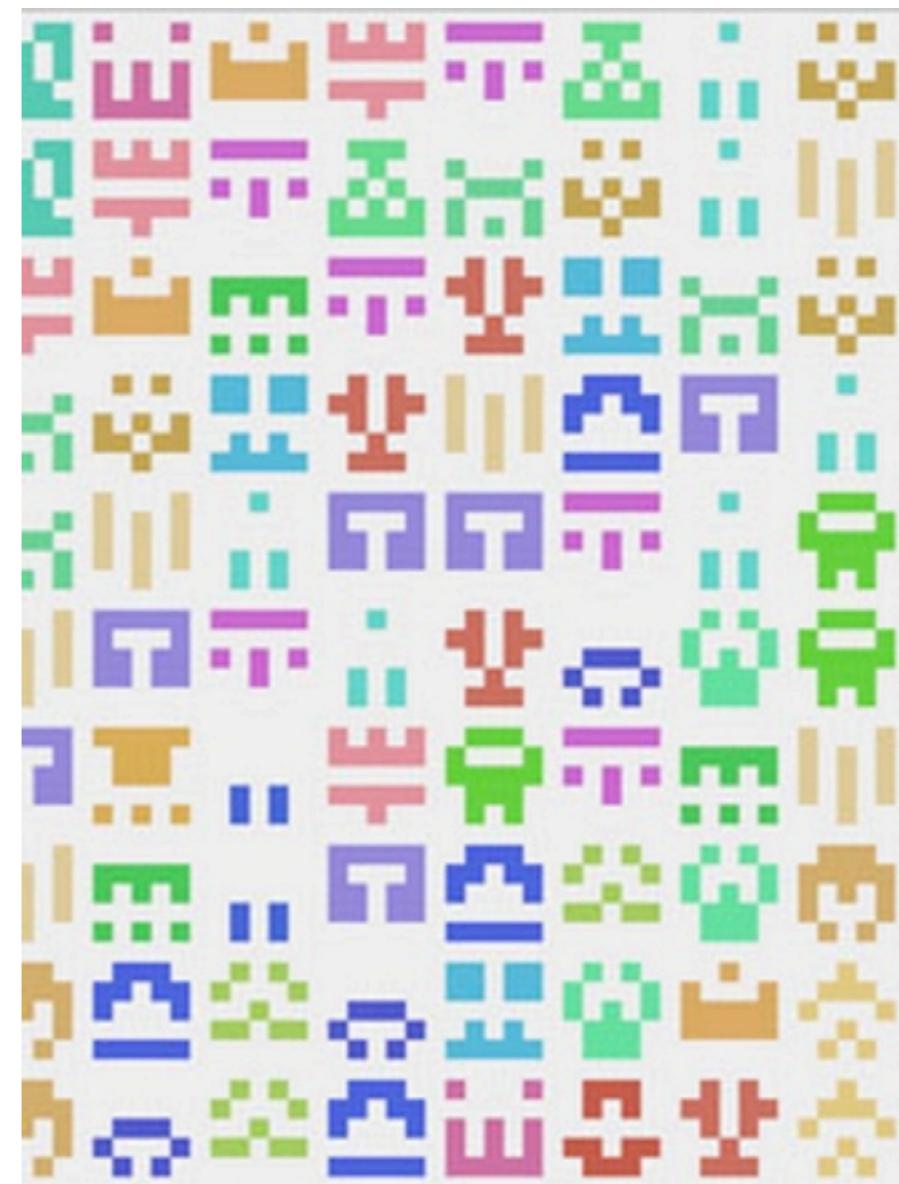
-----END PGP PUBLIC KEY BLOCK-----

Klicken Sie F1, um die Hilfe aufzurufen.



# Everyone has a role

- Activists
- Artists
- Intellectuals
- Regular Americans and world citizens that can weigh in on a social issue



Remind the establishment that no public consensus was ever obtained for PRISM



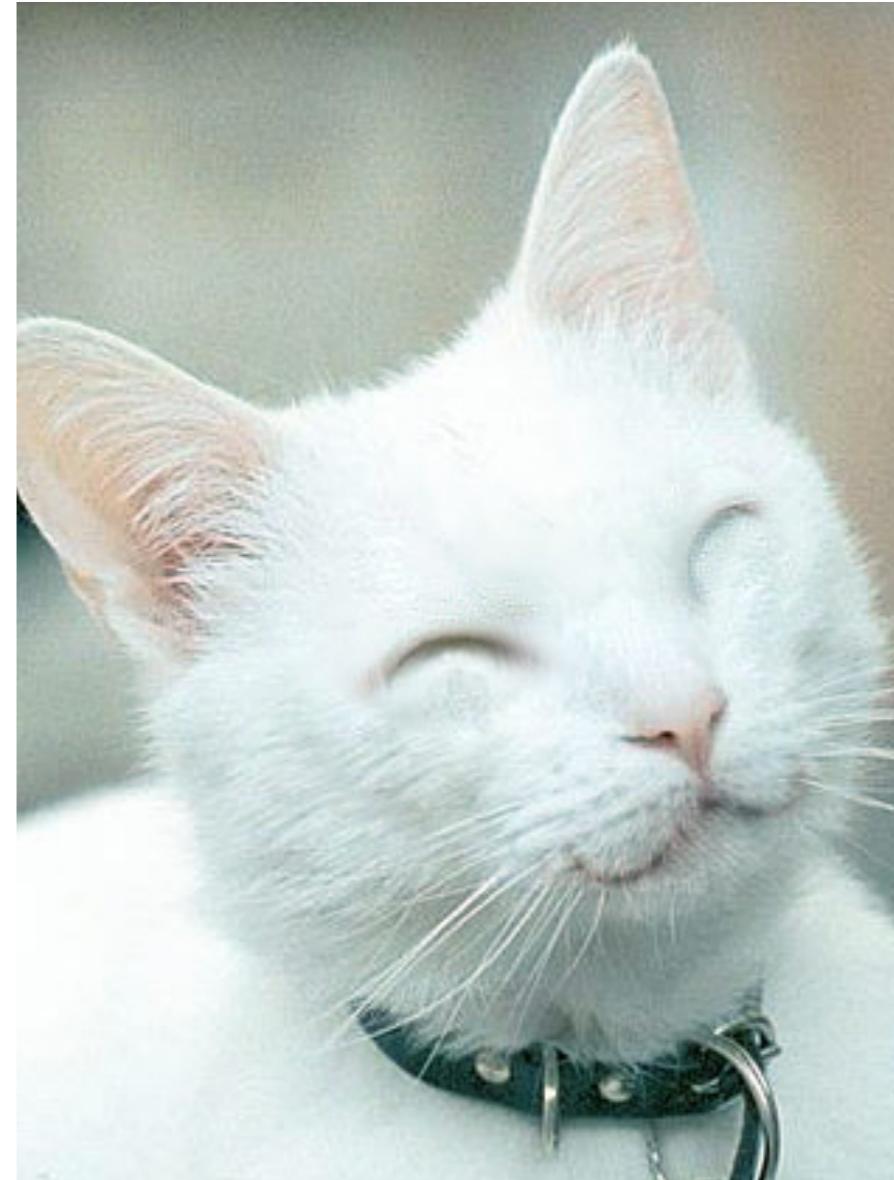
# Dos and don'ts

## Do:

Open up the issue to any  
and all potential victims  
(NRA hates surveillance?  
No problem!)

## Don't:

Make the cause exclusive.





# Dos and don'ts

**Don't:**

Break the law! Political  
legitimacy is crucial.

Good example: EFF

Counter-examples: Anonymous  
takedown of PayPal, etc.





# Dos and don'ts

**Do:**

Invite cooperation from lawmakers, established political groups

**Do:**

Broaden the debate to other mediums





# Dos and don'ts

## Don't:

Stick to technical jargon, or even to the Internet as the only affected medium!

Associating with PIPA/SOPA is good, but broaden your base.





# Dos and don'ts

## Don't:

Marginalize yourself – edge cases should be handled separately, not affect the entire movement



Example: EFF and Bradley/  
Chelsea Manning Defense  
Network

Who has your metadata when you use Cryptocat?	Cryptocat Server	Your ISP
Conversation name	Yes	No
Your nickname	Yes	No
Can see that you are connecting to Cryptocat	Yes <small>(Sees a connecting IP)</small>	Yes <small>(Except if using Tor)</small>
Time messages were sent	Yes	Yes
Which nicknames you are messaging privately/ having file transfers with	Yes	No
Your IP address	Yes <small>(Except if using Tor)</small>	Yes
Contents of conversation	No	No
Contents of file transfers	No	No
Names of files transferred	No	No
Sizes of files transferred	Yes <small>(Approximately)</small>	Possibly
Types of files transferred	Yes	No
Public keys and fingerprints	Yes	No
Private keys	No	No



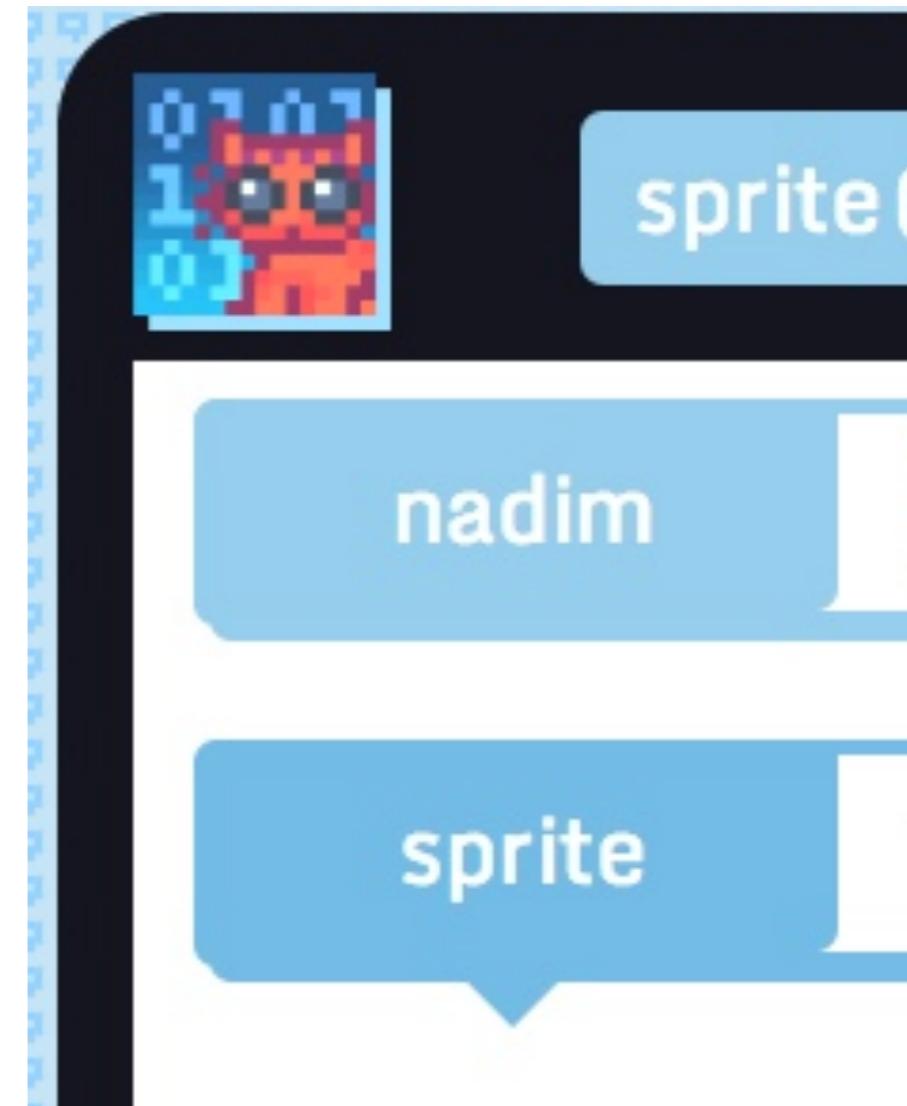


# How does it work?

Download a browser app...

...install it and join a chat!

And that's it.



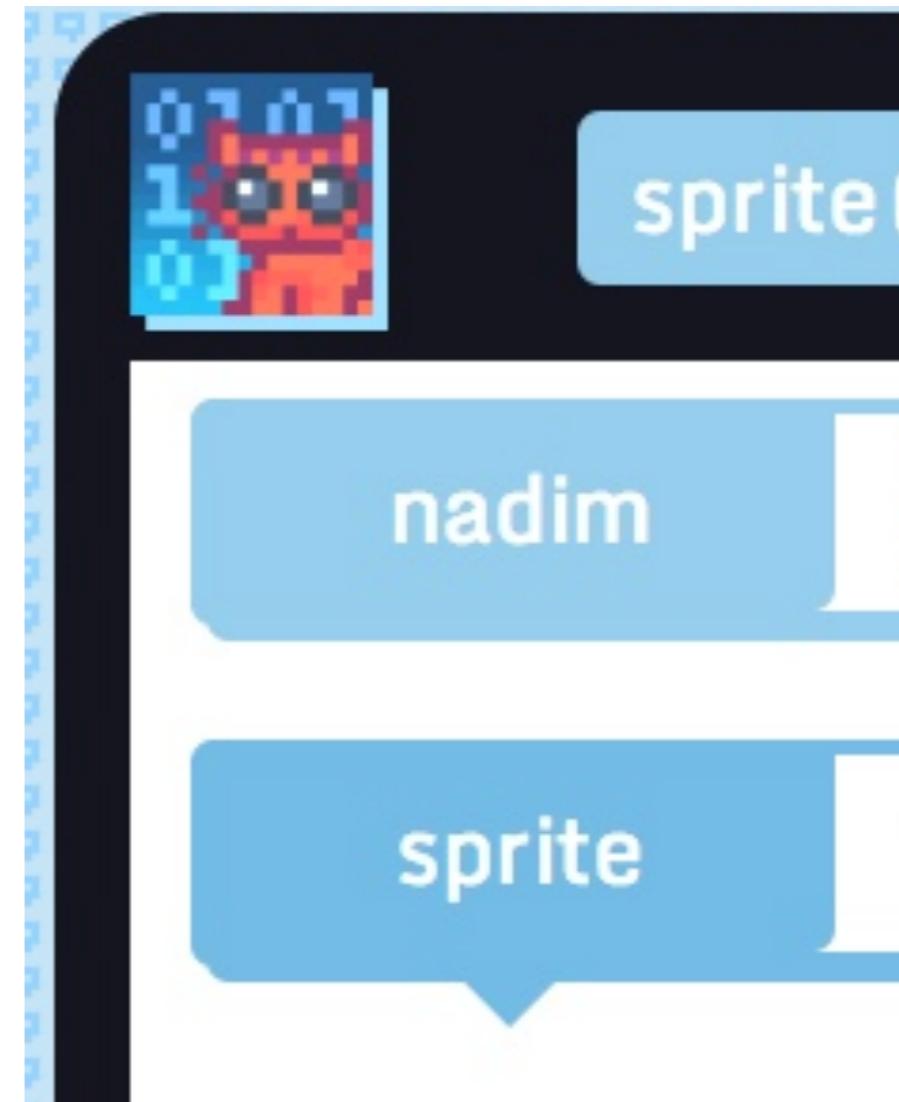


# Usability matters

A colorful, familiar,  
appealing interface...

...accessibility features,  
audio and visual  
notifications...

..and more.





# Challenges in making crypto accessible

Cryptographic  
implementations

Code delivery

Random number generation

...and more.

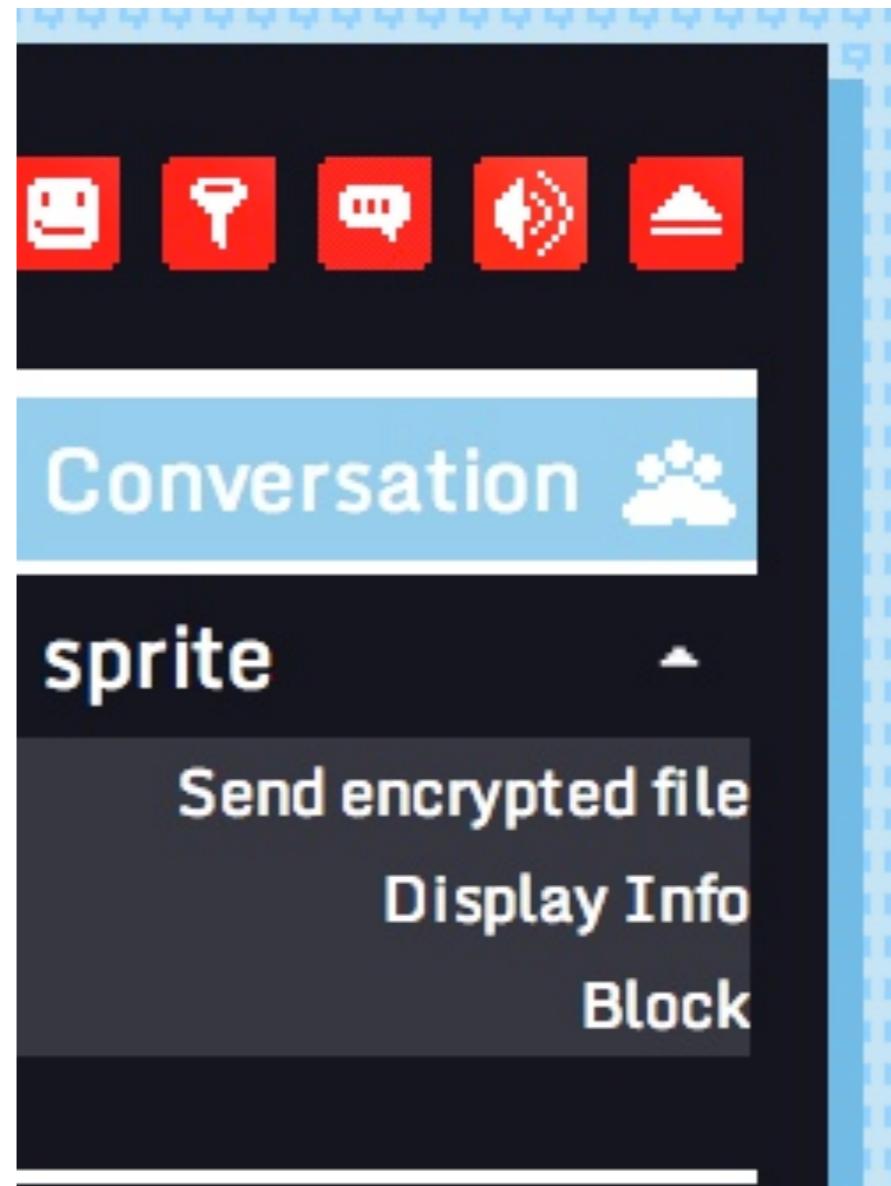




# Is it worth it?

We started in 2011: State of browser crypto almost non-existent.

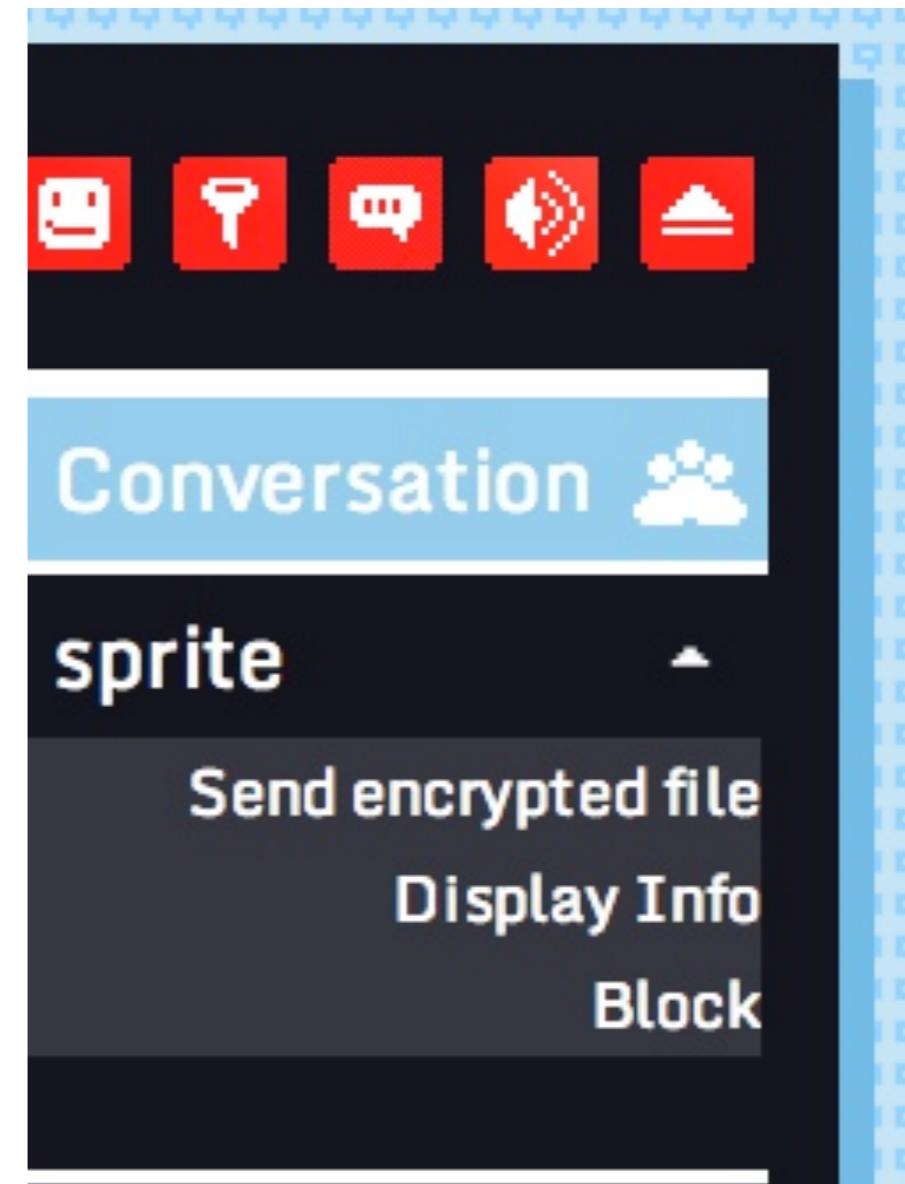
Is it worth it? Are there any real accessibility results?





# So much progress!

Teachers,  
LGBTQ couples,  
Counselors,  
Journalists,  
Friends and family,  
Businesspeople,



Almost **everyone** has found a  
use for accessible privacy.



# Localization matters

Over 35 languages covered.

Cryptocat automatically  
detects browser language,  
configures accordingly.





# Get involved!

Website: [www.crypto.cat](http://www.crypto.cat)

Twitter: @cryptocatapp

IRC: #cryptocat, irc.oftc.net

My email: [nadim@crypto.cat](mailto:nadim@crypto.cat)

