Technological vs. Political Approaches to Surveillance

Nadim Kobeissi

PRISMBreak – New York City

OpenITP
Internet Tools Project

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted]

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

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

[redacted]

April 2013

People today

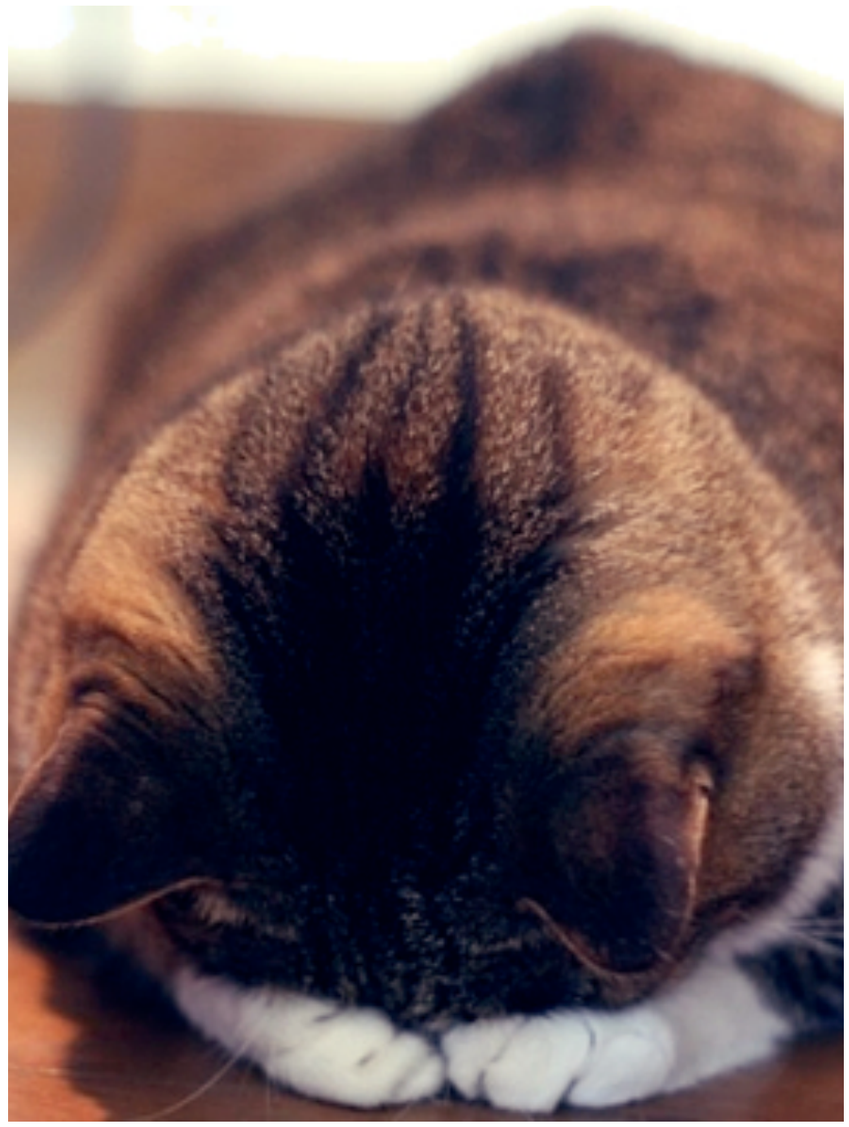
“Let’s solve a global surveillance apparatus built thanks to strong shared realist foreign policy convictions doubled by domestic assurances...

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:

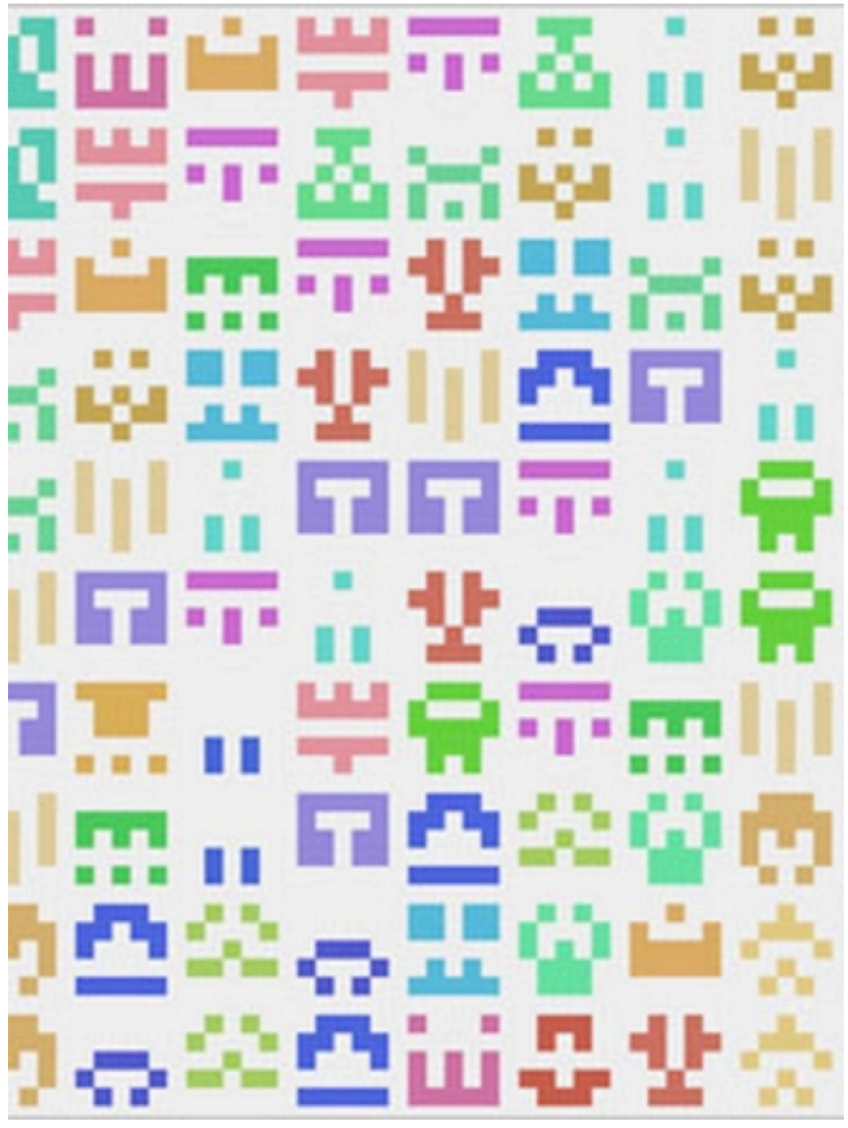
- Research.
- Availability.
- Variety.

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?**

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

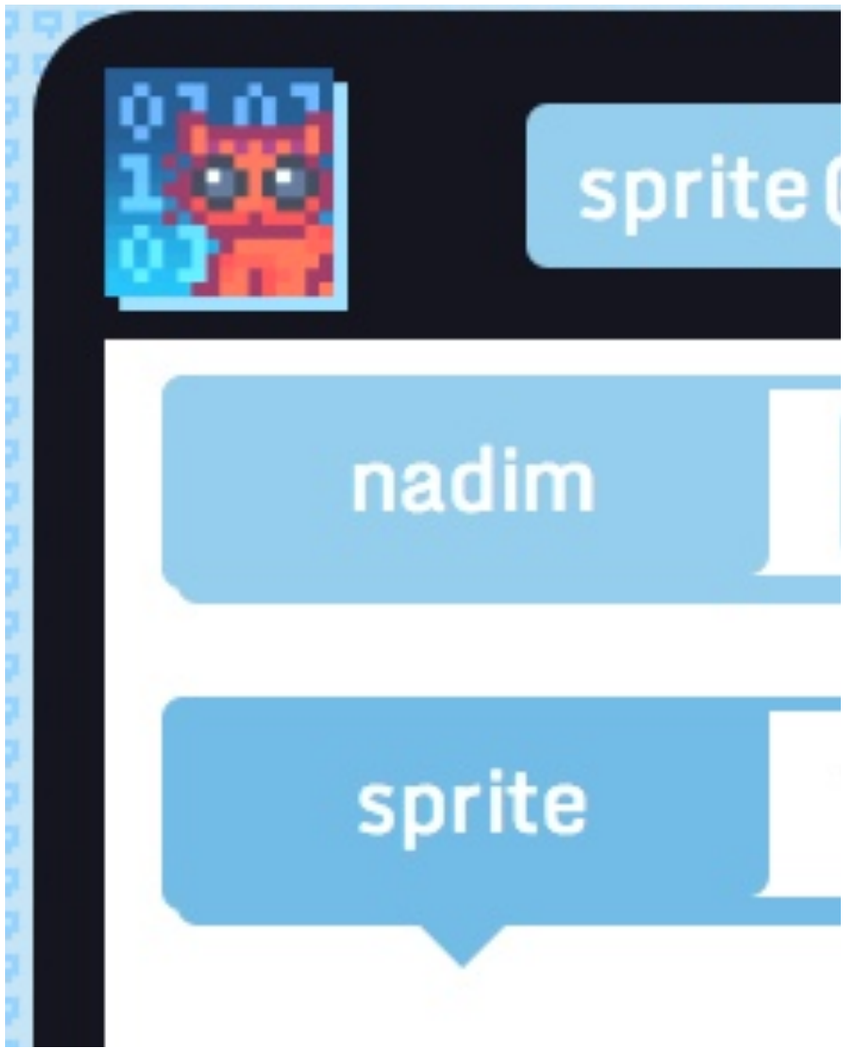
Who has your metadata when you use Cryptocat?	Cryptocat Server	Your ISP
Conversation name	**Yes**	**No**
Your nickname	**Yes**	**No**
Can see that you are connecting to Cryptocat	**Yes** (Sees a connecting IP)	**Yes** (Except if using Tor)
Time messages were sent	**Yes**	**Yes**
Which nicknames you are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

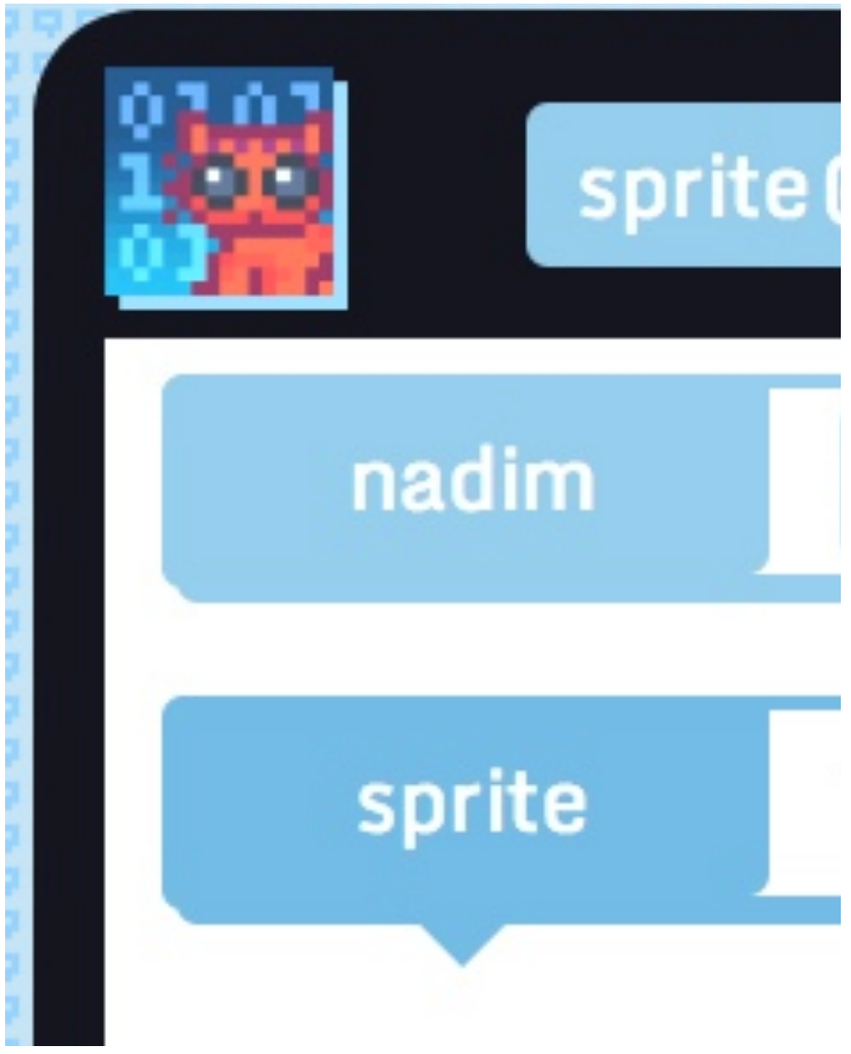
...install it and join a chat!

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

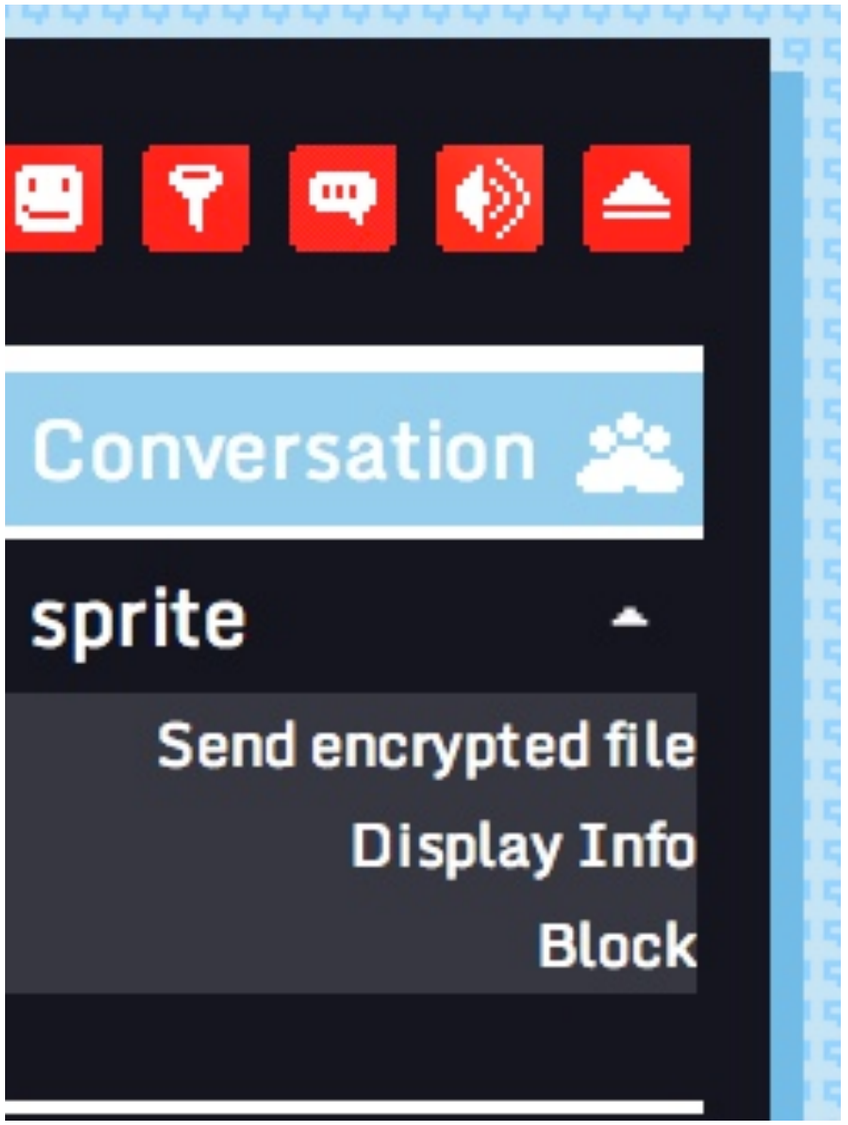
Random number generation

...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,

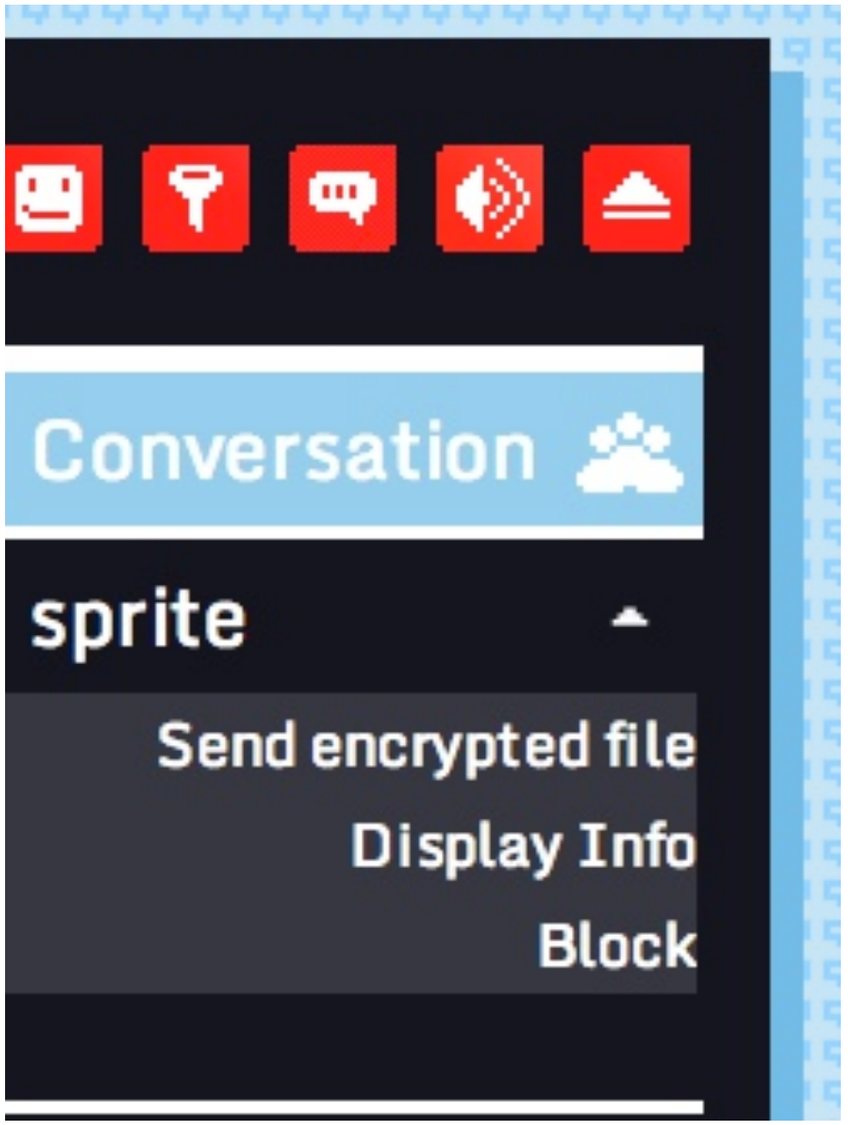
LGBTQ couples,

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

Twitter: @cryptocatapp

IRC: #cryptocat, irc.oftc.net

My email: nadim@crypto.cat