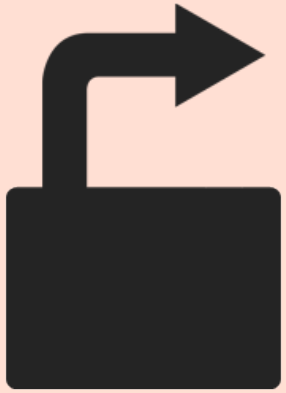


The Open Privacy Stack: Privly

@privly

Lead Developer: Sean McGregor @seanmcgregor

Community Manager: Jennifer Davidson @jewifer

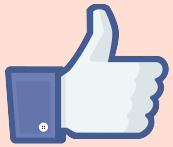
Outline

1. How the web is broken for security
2. "Injectable Applications" as a solution
3. How Privly implements injectable applications
4. More on injectable applications
5. The Privly Foundation and the way forward

How Security on the Web is Broken

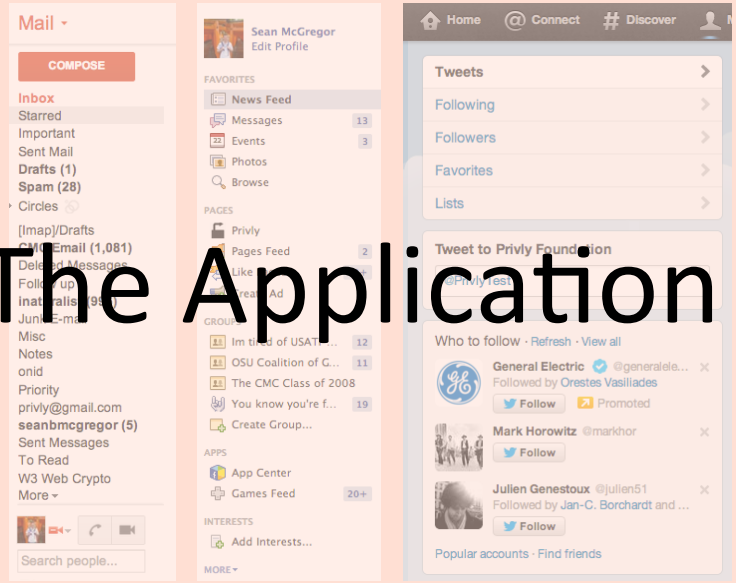
PRISM: Online service providers cannot protect users from the governments under which they operate

Hushmail: Online services cannot protect users from themselves



Facebook "Like" Button: Security and functionality are difficult to combine

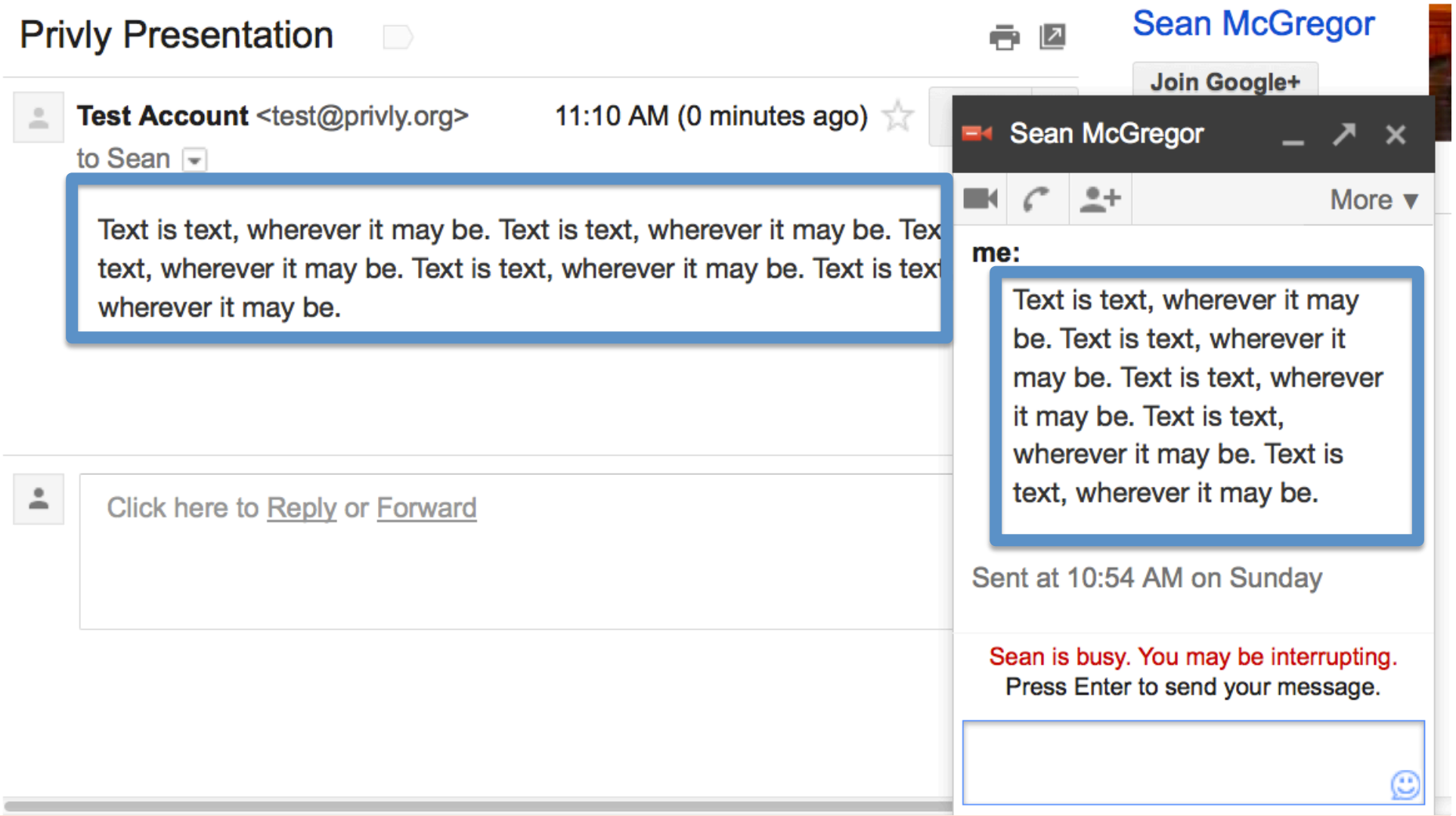
Solution: Stop Reinventing Security



The Application !== The Data

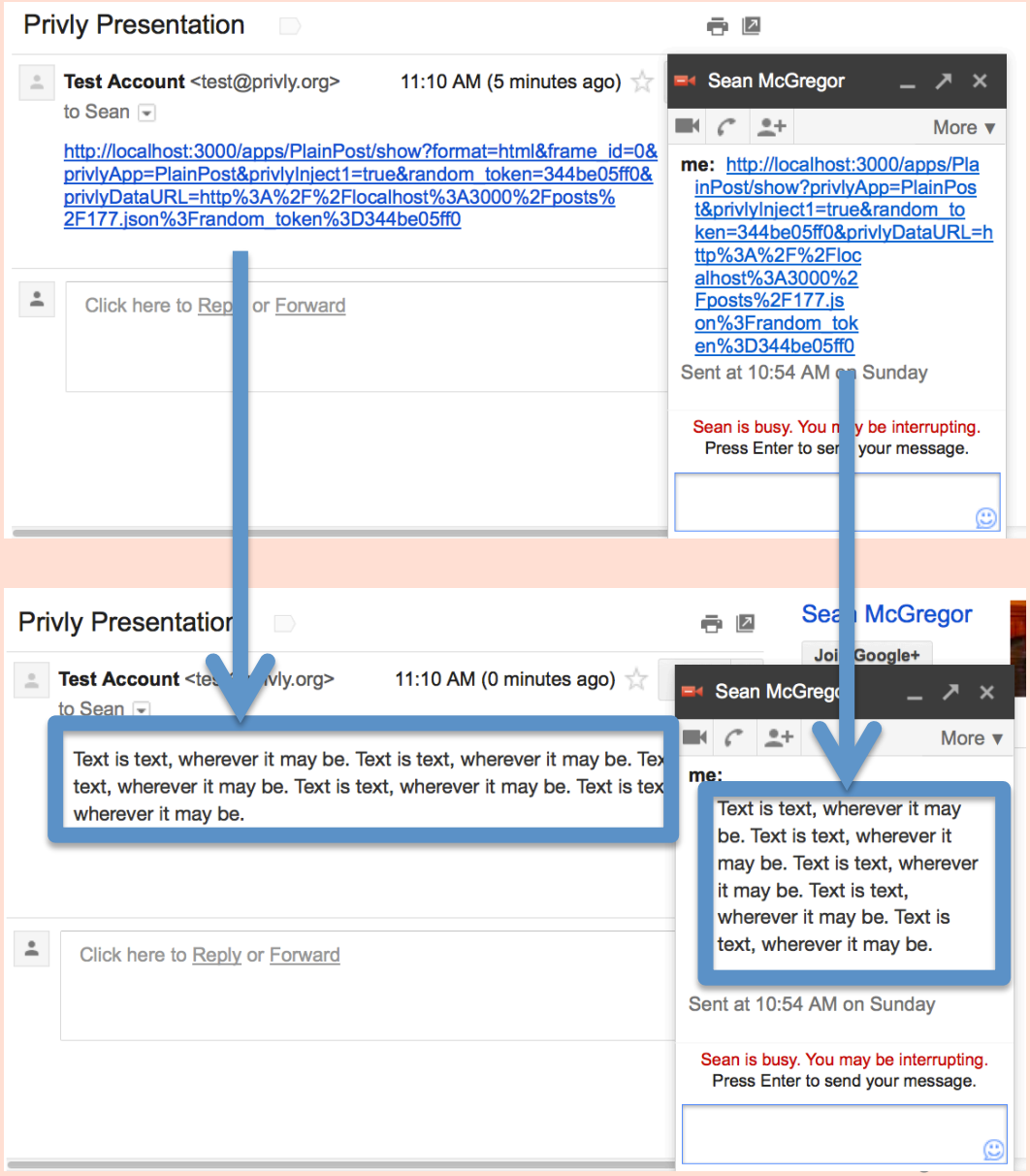
- Your site is unique, but your data is not!
- Wrap content in its own application viewed inside your web application

Text is Text, Wherever it May Be

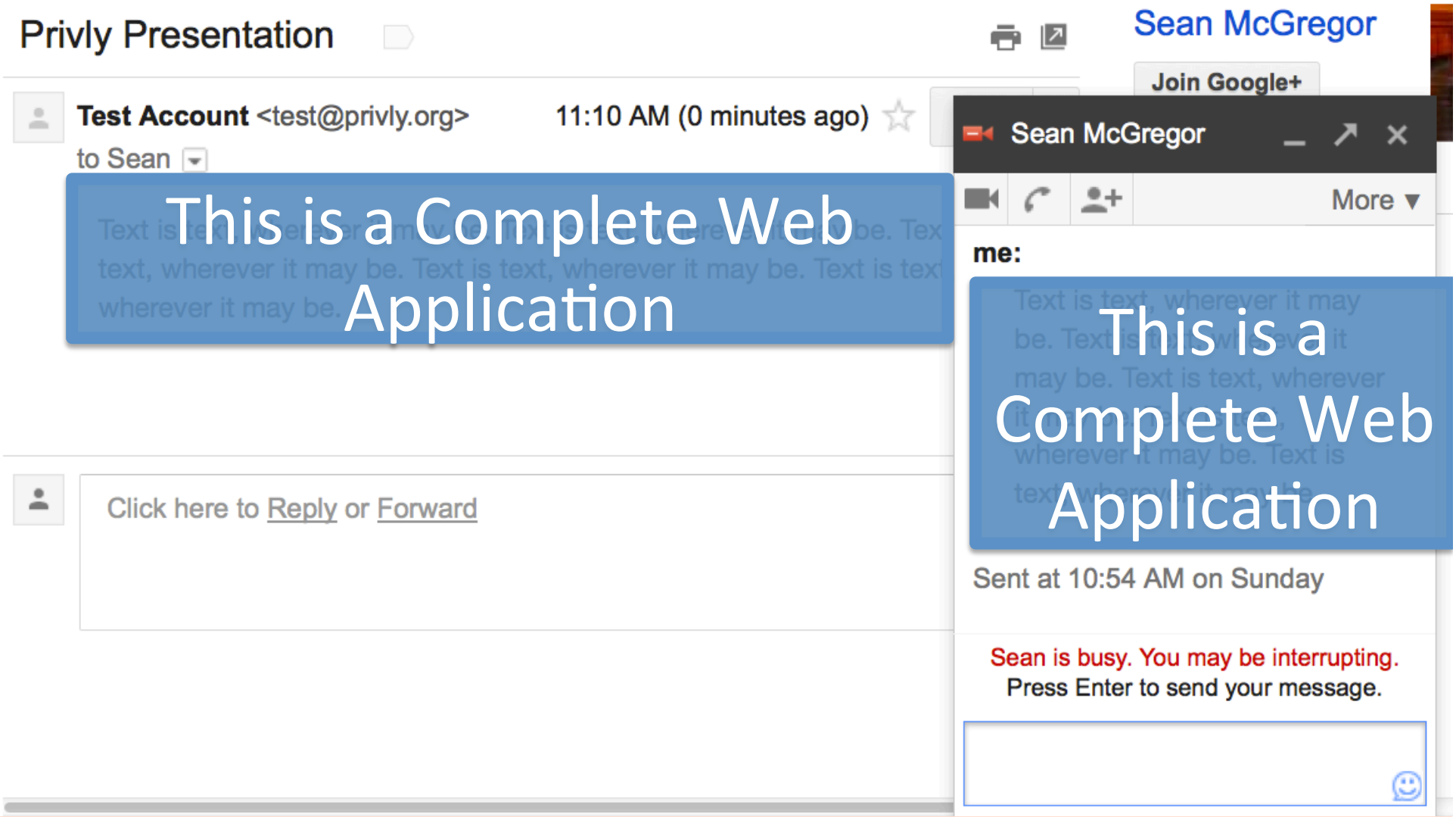


That Was Privly at Work

1. Browser Extension discovers specially formatted link
2. “Injects” the link



Text is Text, Wherever it May Be



The Privly URL

privlyApp=PGP

privlyApp=ZeroBin

privlyalpha.org/apps/PlainPost?privlyApp=PlainPost&privlyDataURL=privlyalpha.org/posts/1.json

1
The hosted app path

2
App specifier

3
Data address

https://Privlyalpha/apps/PlainPost?privlyApp=PlainPost&privlyDataURL=https://privlyalpha.org/posts/2342536674.json

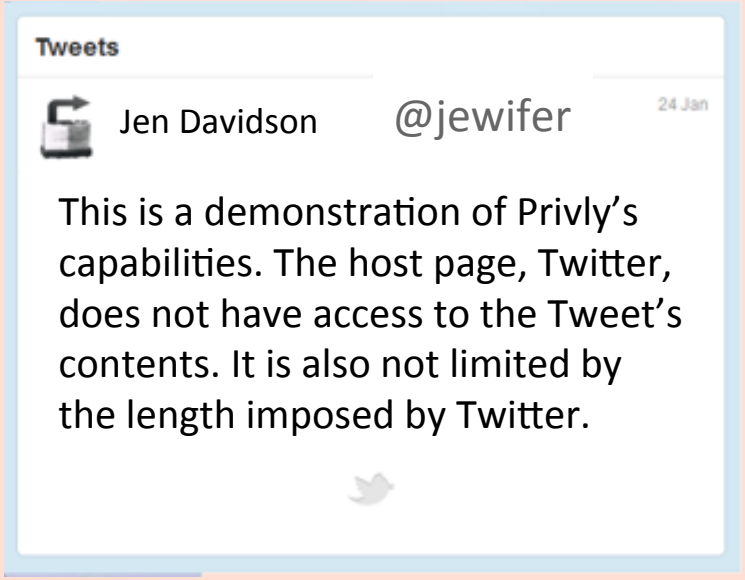
This is a demonstration of Privly's capabilities. The host page, Twitter, does not have access to the Tweet's contents. It is also not limited by the length imposed by Twitter.

-47 Tweet

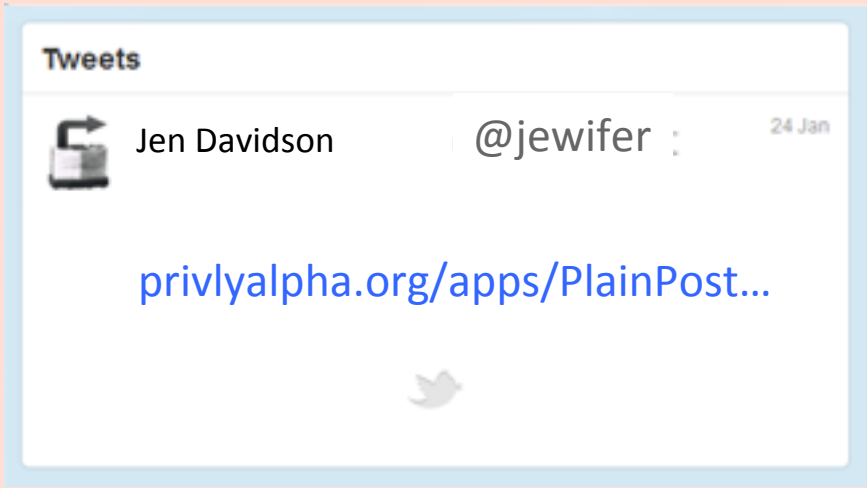
Extended Browser

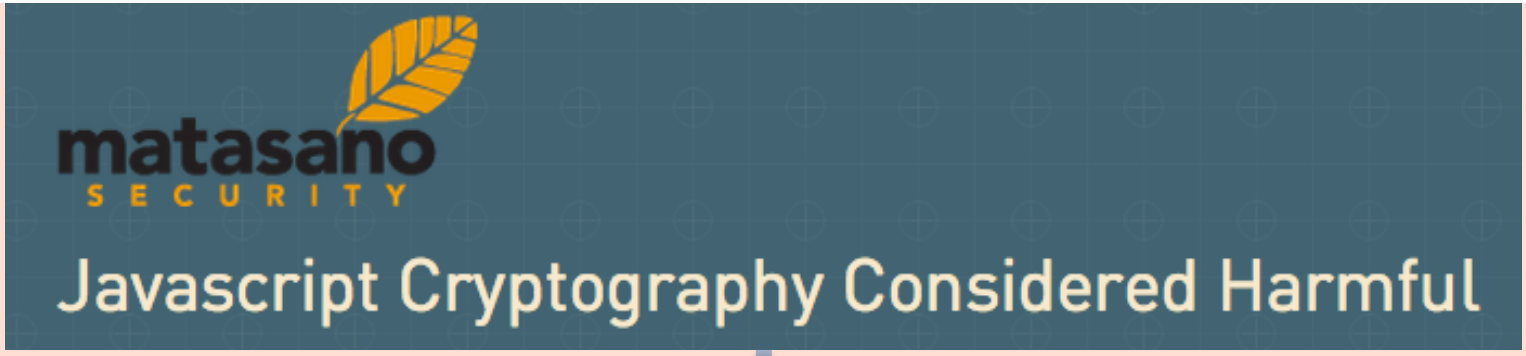
Host Page

Extension



No Extension





?privlyApp=PlainPost&

2

App specifier

Pre-Distribute the Apps

Privly

Javascript Cryptography **Potentially** Not Harmful

What if the User Doesn't Have the App?

privlyalpha.org/apps/ZeroBin

1

The hosted app path

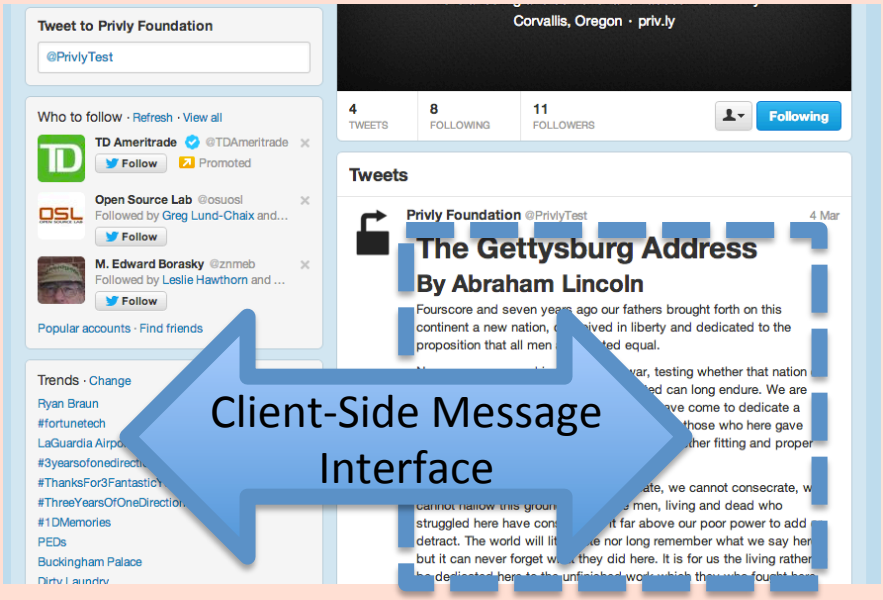
- Optional hosted fallback
  - Posting users can choose an app where hosted fallback is possible
  - You do not protect users from the host
  - Best case, you host it yourself
  - ZeroBin App is a compromise

More About these “Injectable Apps”

- Current
  - PlainPost: Most universal application
  - ZeroBin: Encrypted by the anchor text
- In Development
  - PGP: Strong Public Key Crypto
  - IndieData: Personal Semantic Datastore
- Planned
  - OTR: Encrypted chat application
  - various other specific use cases

Cool Potential Functionality

- Host page API
- Hooks into distributed hash table
- Seamless integration with social networks for sharing lists



Are Websites the Adversary?

- Only from a security perspective
  - Have to account for worst case scenarios
- Privly increases time-on-site
  - Increased add revenues
  - Time-on-site is more valuable than being able to target advertising to private message contents

Privly Development Status

- Google Chrome Extension is the most advanced
- Use the Chrome Extension to develop Injectable Apps
- Google Summer of Code students are developing iOS and Android version

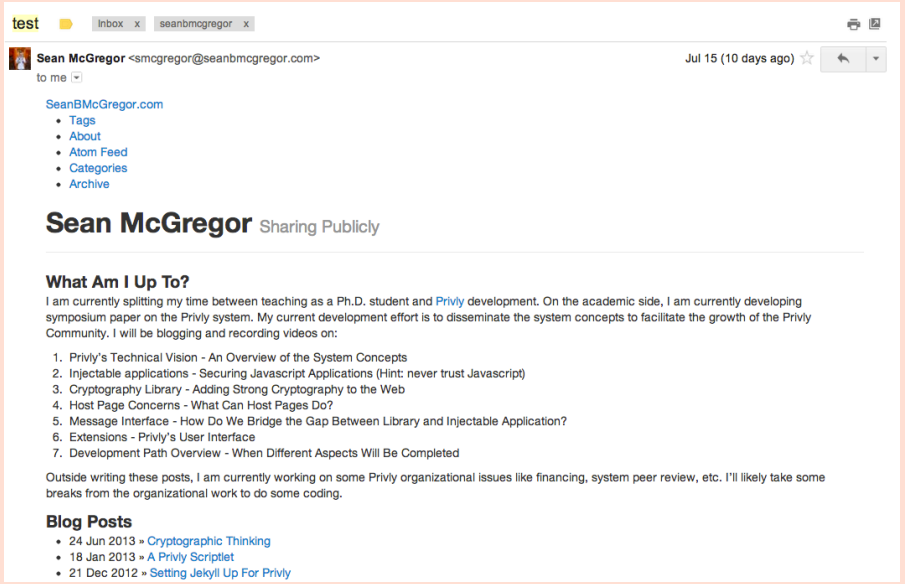
Content Servers

Sophistication

GitHub Pages

BACKBONE.JS

- Data driven
- Advertises extensions
- Privly-applications runs from static folder


test Inbox x seanbmcgregor x

Sean McGregor <smcgregor@seanbmcgregor.com> Jul 15 (10 days ago)
to me

SeanBMcGregor.com
- Tags
- About
- Atom Feed
- Categories
- Archive

Sean McGregor Sharing Publicly

What Am I Up To?

I am currently splitting my time between teaching as a Ph.D. student and Privly development. On the academic side, I am currently developing symposium paper on the Privly system. My current development effort is to disseminate the system concepts to facilitate the growth of the Privly Community. I will be blogging and recording videos on:

1. Privly's Technical Vision - An Overview of the System Concepts
2. Injectable applications - Securing Javascript Applications (Hint: never trust Javascript)
3. Cryptography Library - Adding Strong Cryptography to the Web
4. Host Page Concerns - What Can Host Pages Do?
5. Message Interface - How Do We Bridge the Gap Between Library and Injectable Application?
6. Extensions - Privly's User Interface
7. Development Path Overview - When Different Aspects Will Be Completed

Outside writing these posts, I am currently working on some Privly organizational issues like financing, system peer review, etc. I'll likely take some breaks from the organizational work to do some coding.

Blog Posts
- 24 Jun 2013 » Cryptographic Thinking
- 18 Jan 2013 » A Privly Scriptlet
- 21 Dec 2012 » Setting Jekyll Up For Privly

OSCON 2013

priv.ly/pages/download

What's Next

- Security is hard, innovation is **dangerous**
- Put warnings on **everything** and release/ iterate

Making an Injectable Application

- Start with the Chrome extension: github.com/privly/privly-chrome
- Easiest way to start is by editing the PlainPost application

Resources

- Info/Download: priv.ly
- Communicate: privly.org
- Code: https://github.com/privly
- Latest Content Server: https://privlyalpha.org
- Slides: github.com/privly/privly-organization/tree/master/presentations/2013-07-25-OSCON/OSCON.ppt

Get Connected

#privly on irc.freenode.net

Join our mailing list, http://bit.ly/privly-group

Techno-Activism 3rd Mondays

- August Event: http://ta3m-pdx-3.eventbrite.com
- TA3M Wiki: http://wiki.openitp.org/events:techno-activism_3rd_mondays

Free (As in Beer)

- The handouts at the front have directions for getting credentials on on privlyalpha.org

Wait…what?

- Privly allows you to post “private” content anywhere on the web
- Privly allows you to offer your users protection from your servers (because what if they get compromised? Onooo!)
- Privly is a flexible framework – you can add all kinds of applications

Legal

- All logos are property of their respective owners
- Graphics in this presentation are used under a Creative Commons License
- This presentation is licensed under Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) (http://creativecommons.org/licenses/by-sa/3.0/)

Questions?

Thanks to O'Reilly Media!

https://priv.ly

https://groups.google.com/group/privly

@privly

Sean: @seanmcgregor

Jen: @jewifer

Extra Time Resources

Kickstarter

Our Kickstarter Experience

REFERRERS

Dollars pledged via Kickstarter

$8,814

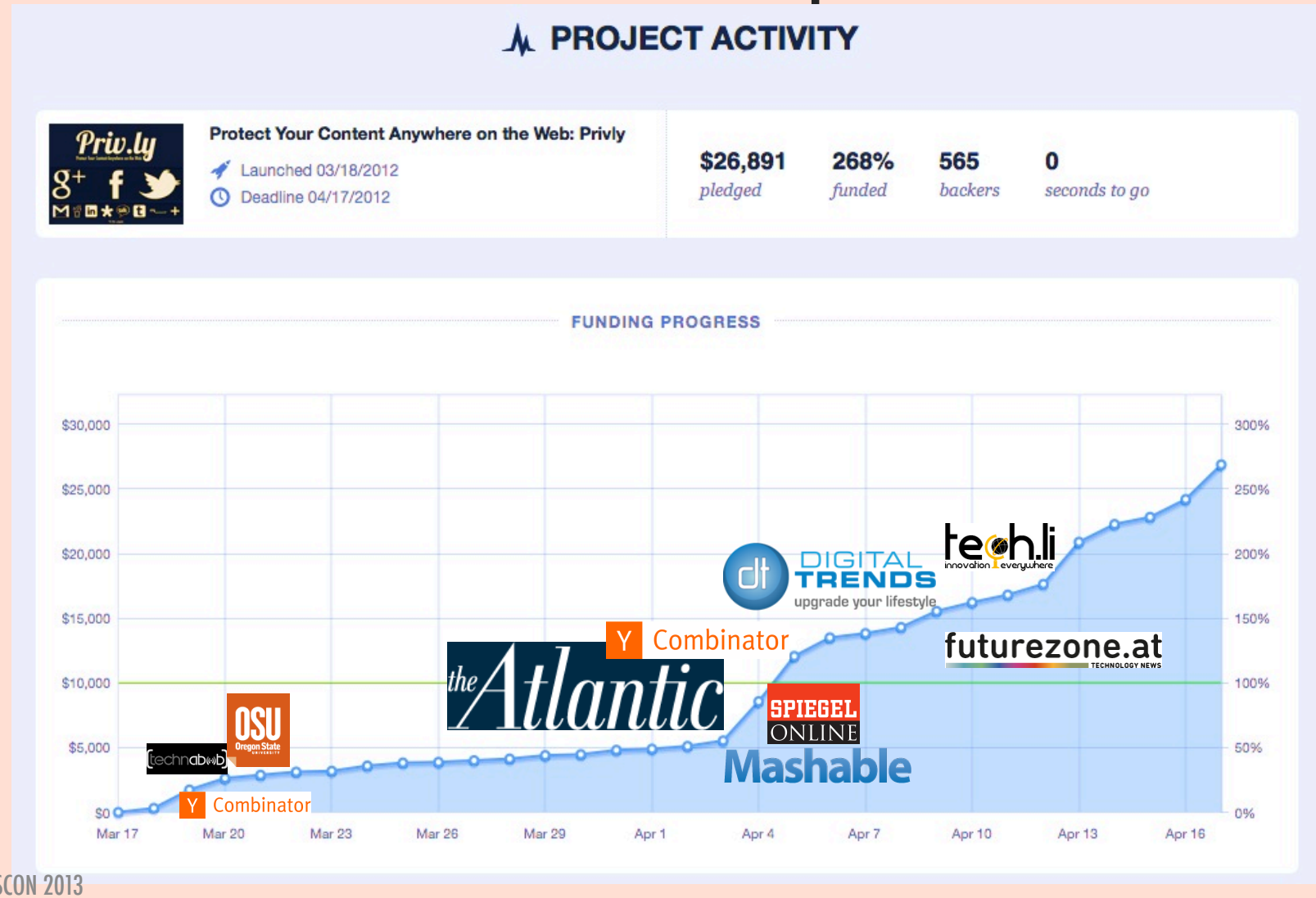
Dollars pledged via external referrers

$18,077

Average pledge amount

$47.60

Kickstarted in April 2012



OSCON 2013

priv.ly/pages/download

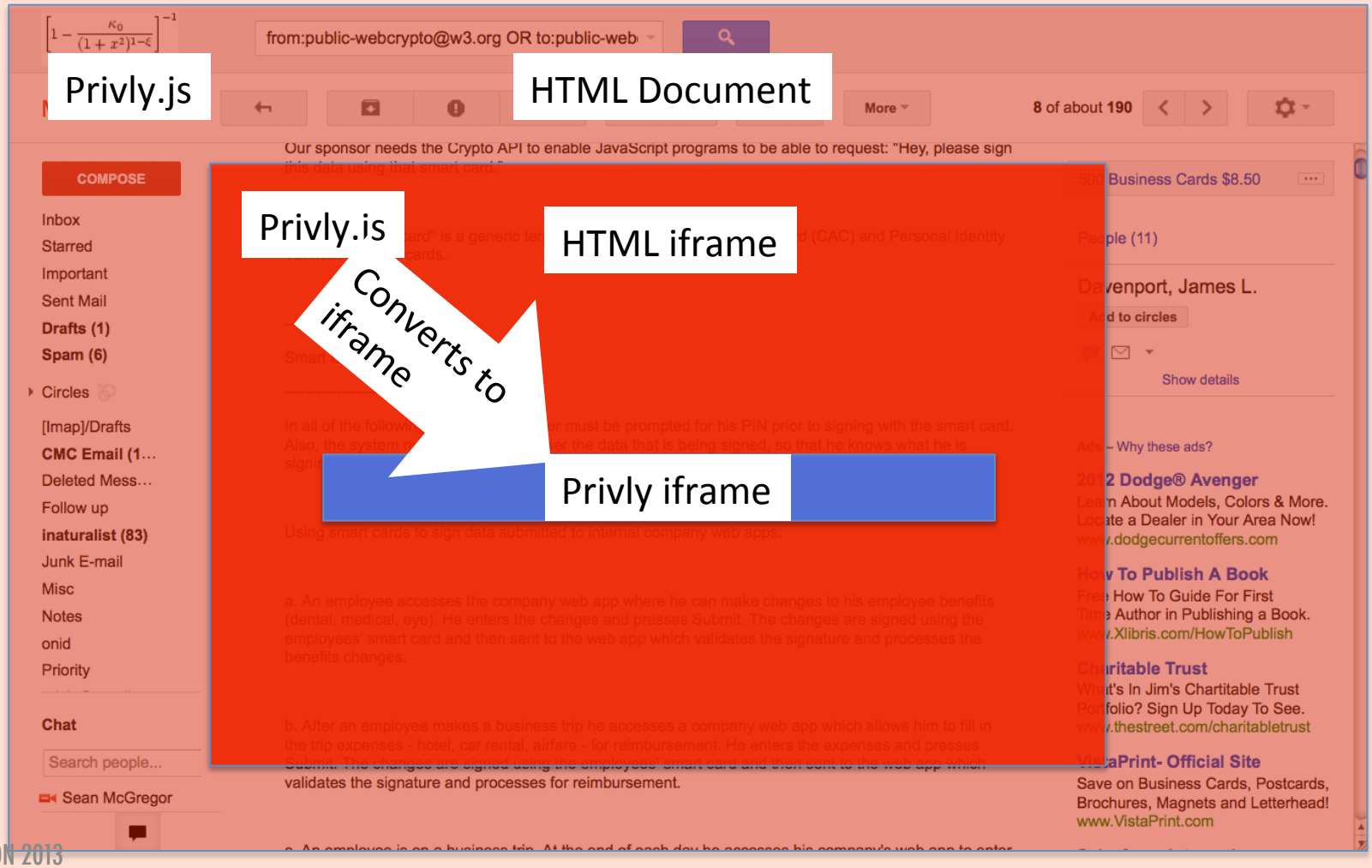
Sell

A Product -Or- A Cause

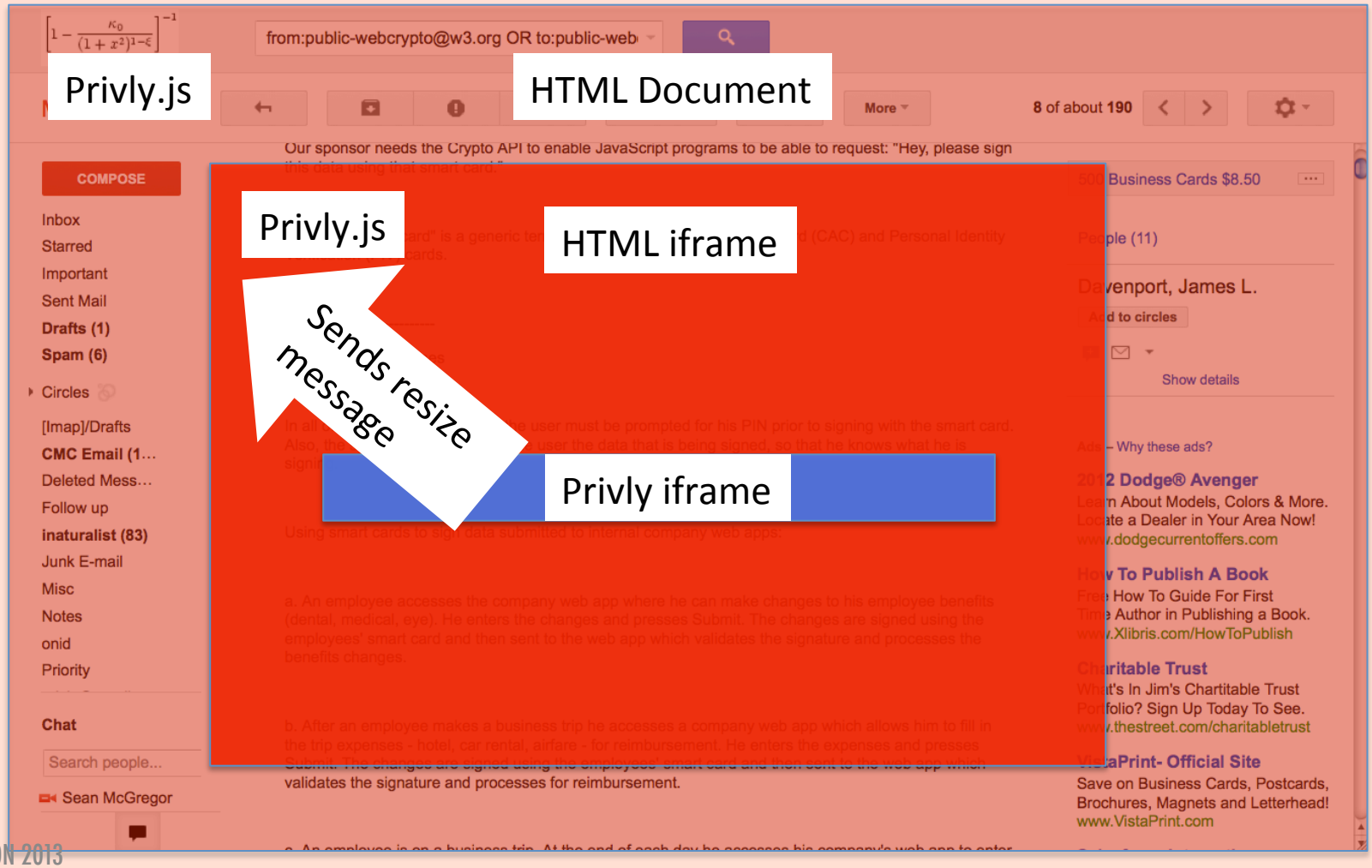
SLIDES WE MAY USE

- SLIDES WE MAY USE

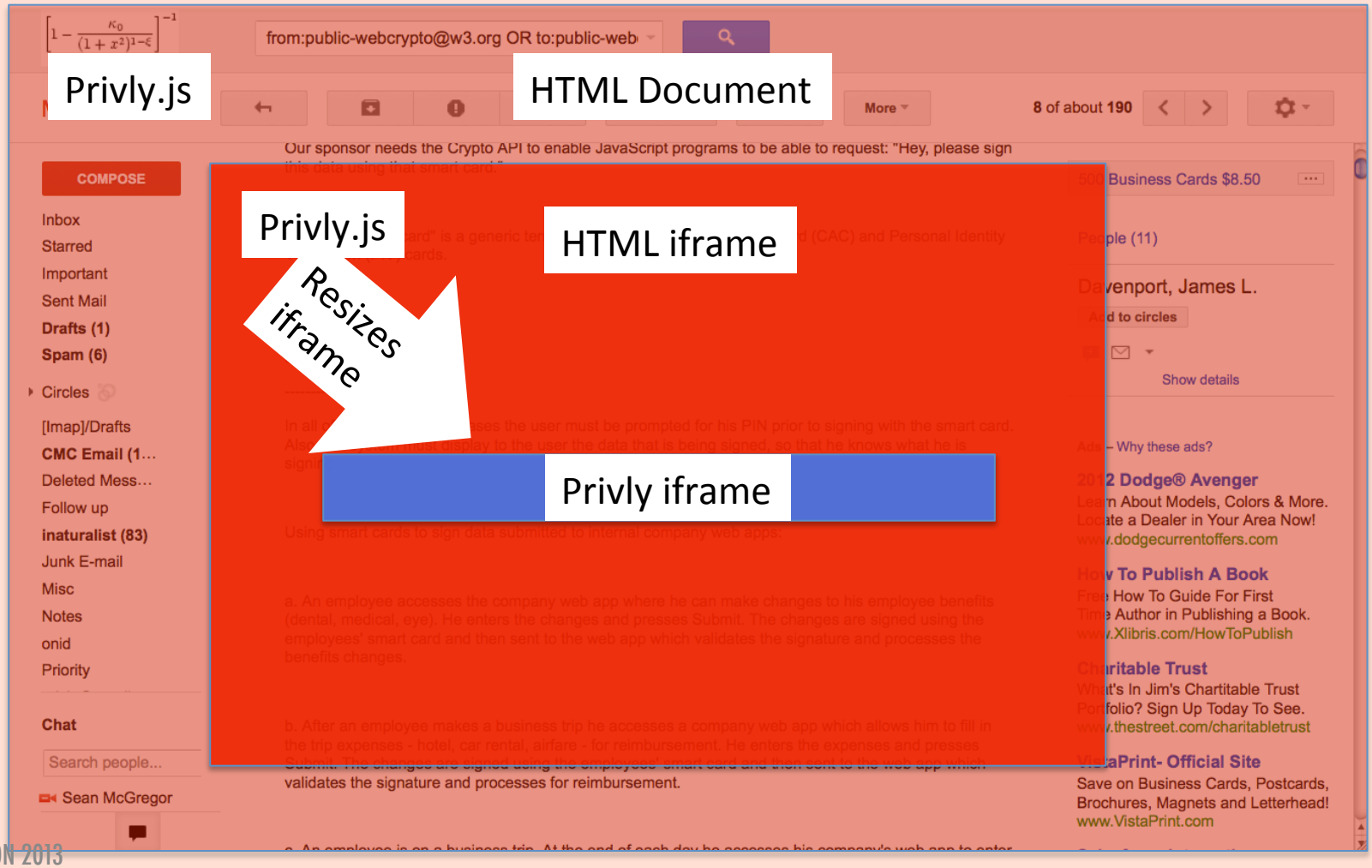
Host Page Script: privly.js



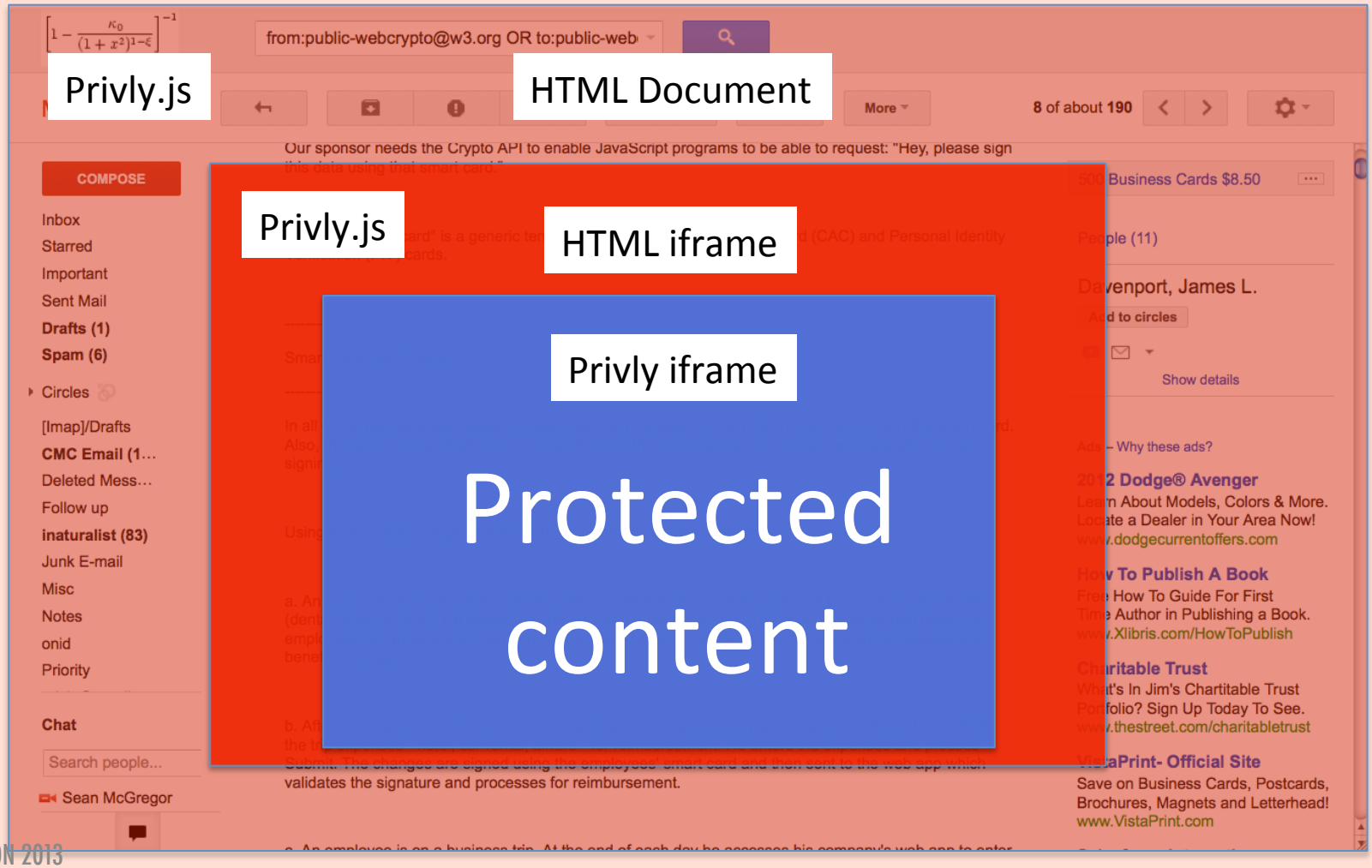
Host Page Script: privly.js



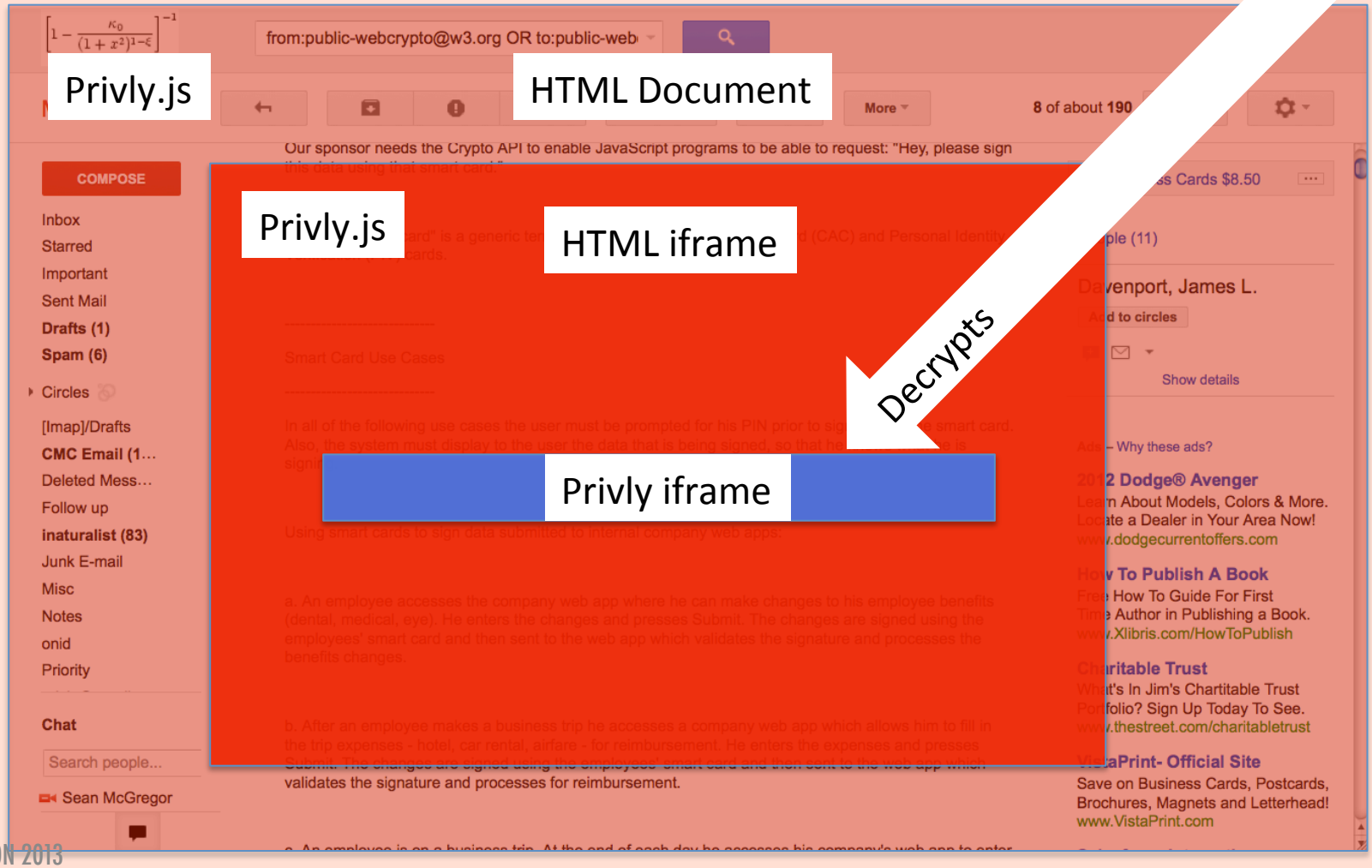
Host Page Script: privly.js



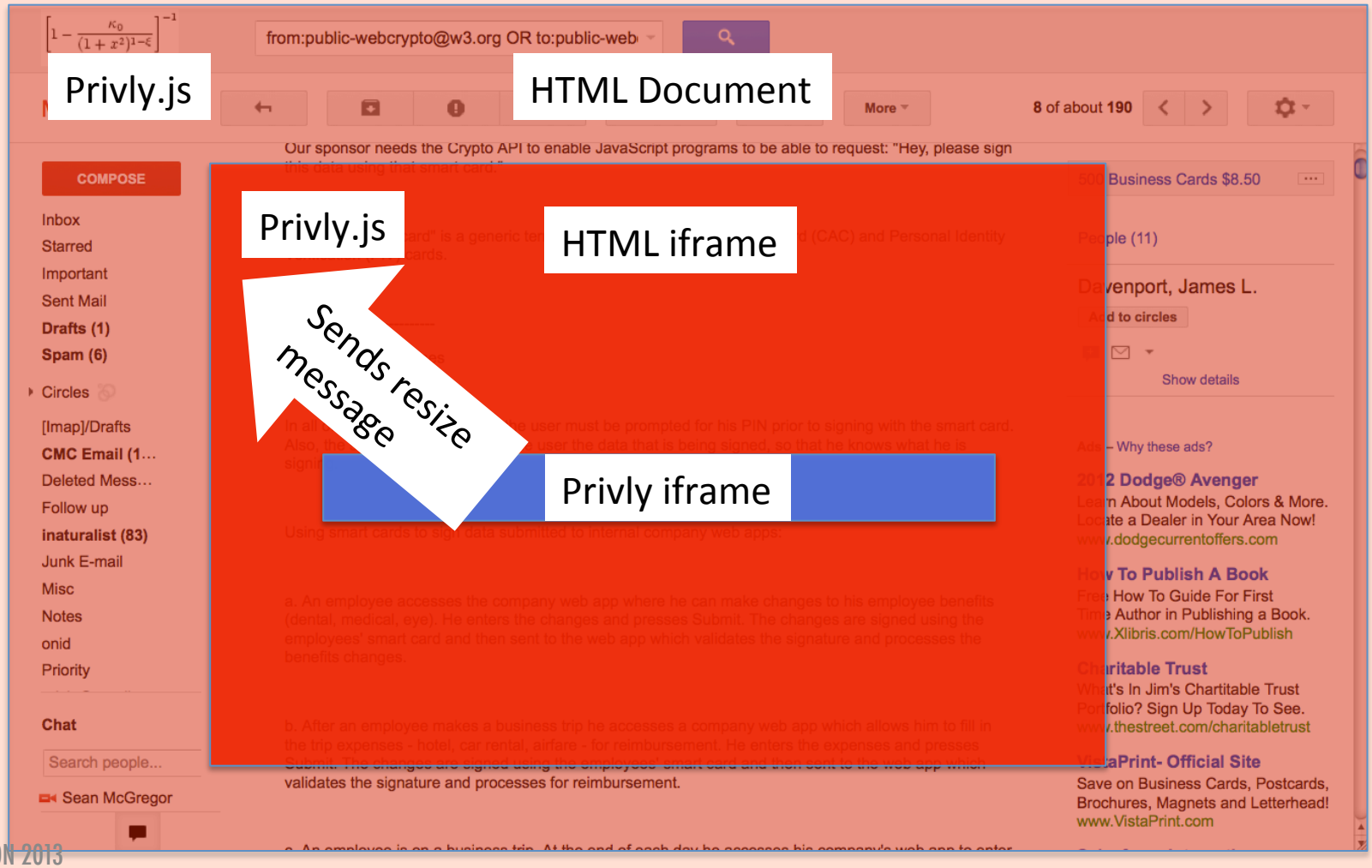
Host Page Script: privly.js



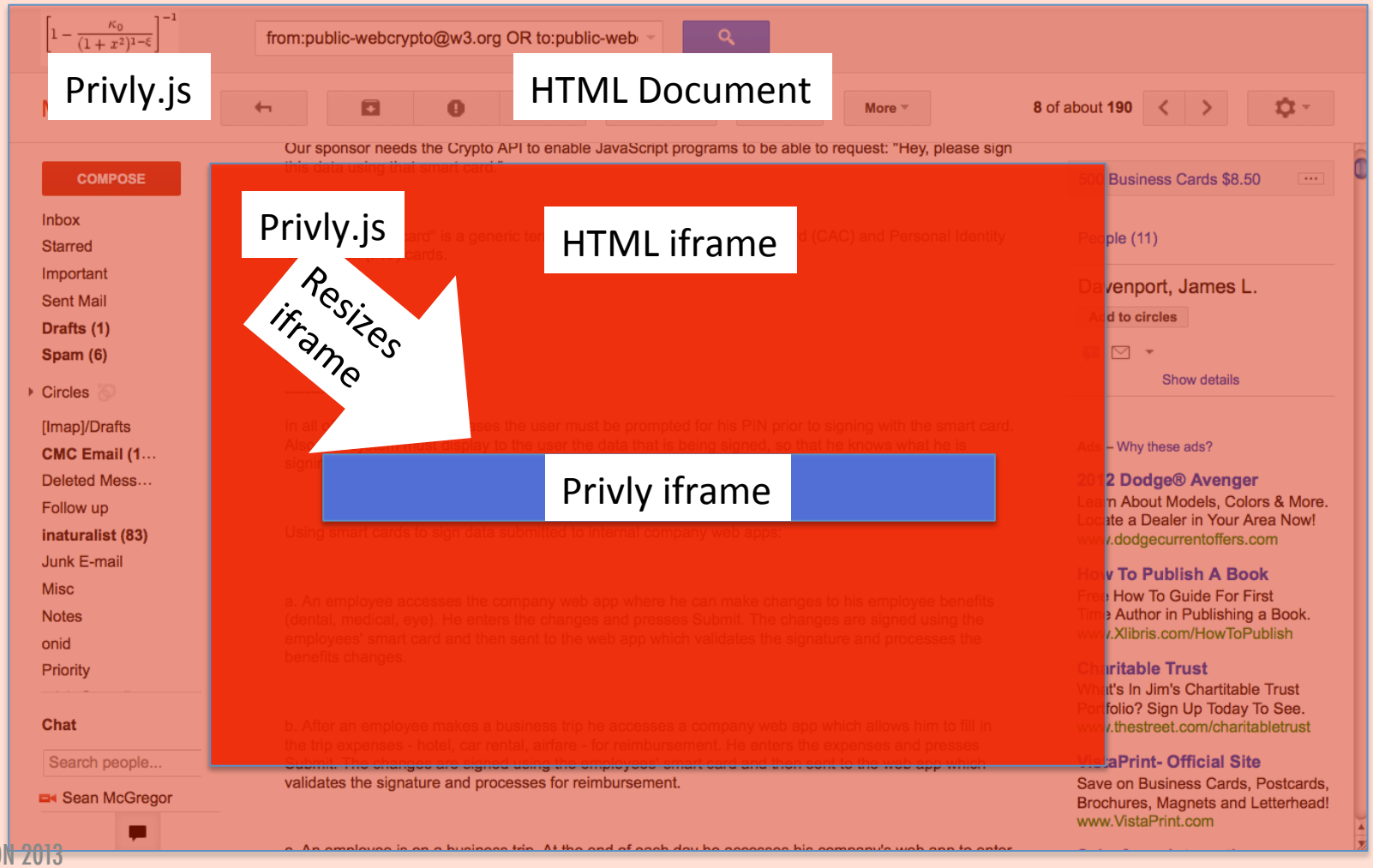
Extension Level: Decryption



Extension Level: Decryption



Extension Level: Decryption



Extension Level: Decryption