ThoughtWorks®

Our Responsibility to Defeat Mass Surveillance

Erik Dörnenburg

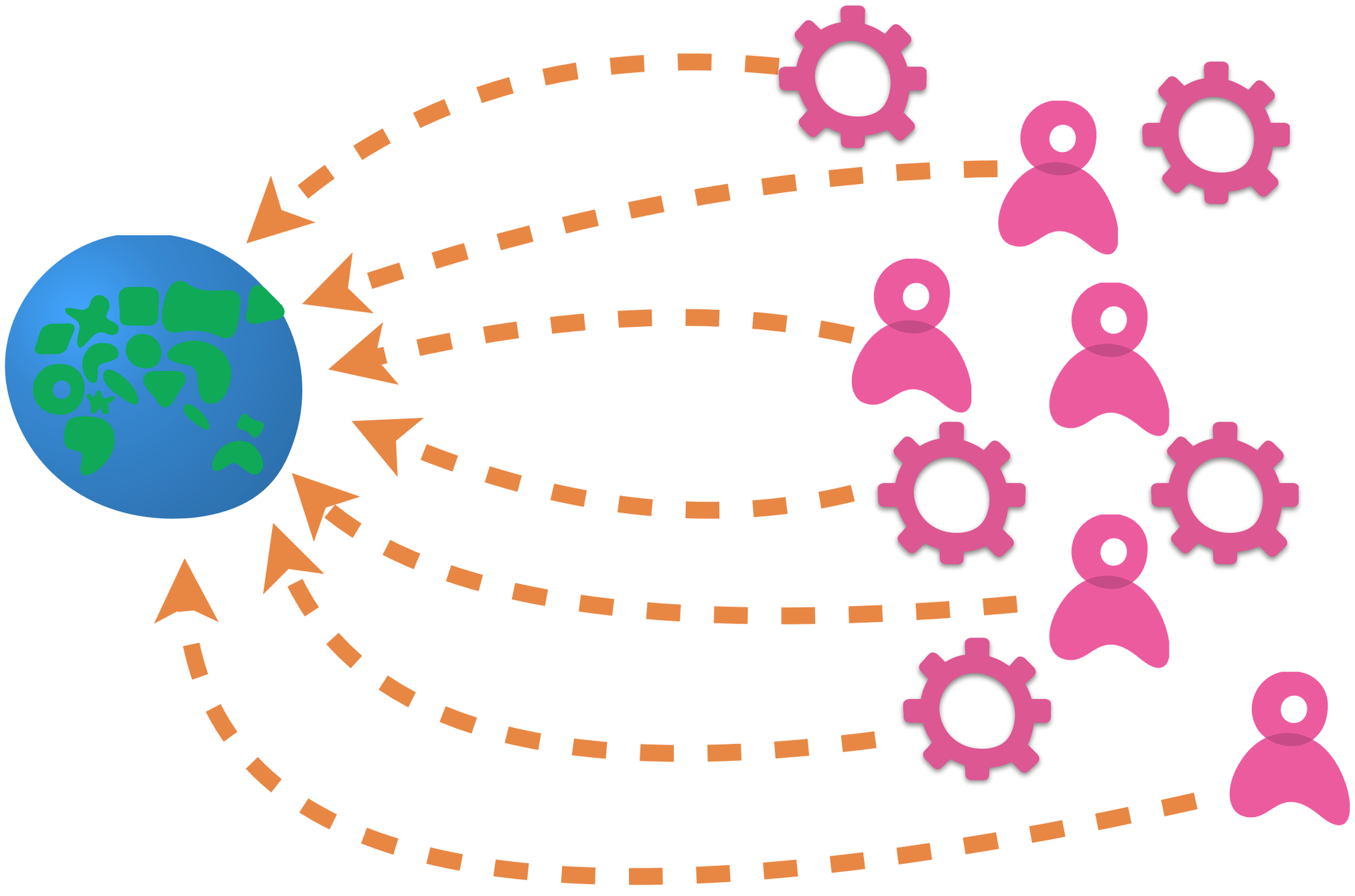
http://erik.doernenburg.com
@erikdoe
http://thoughtworks.com/de

Martin Fowler

http://martinfowler.com
@martinfowler
http://thoughtworks.com

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinised.

~ George Orwell, 1984 (fifth paragraph)



Strong Privacy

Enough?

$$$$$$$$$$$$$$$$$$$$$$$$$$$
$$$$$$$$$$$$$$$$$$$$$$$$$$$
Stop mostly everyone
$$$$$$$$$$$$$$$$$$$$$$$$$$$
$$$$$$$$$$$$$$$$$$$$$$$$$$$

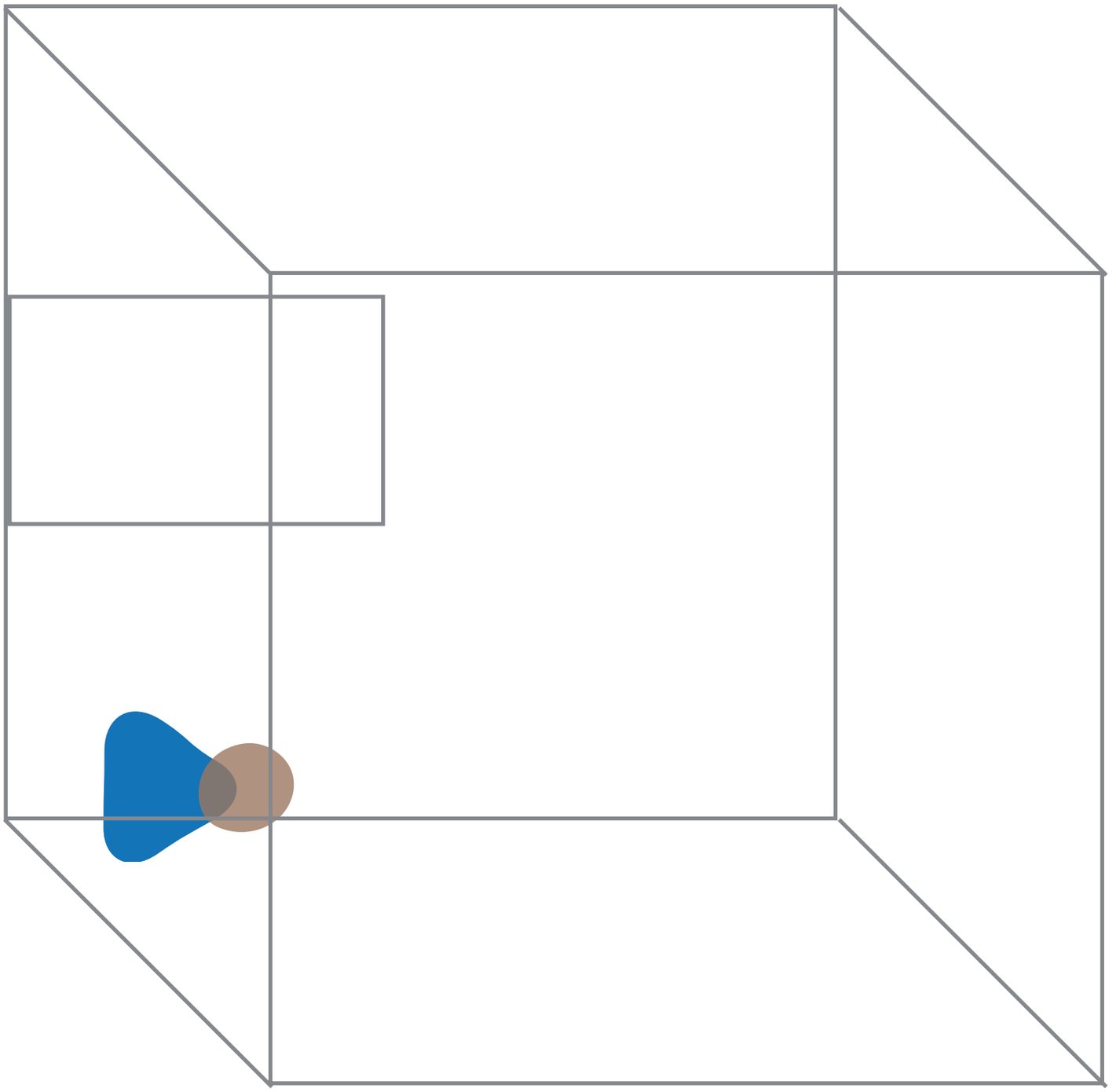
Common Privacy

$$$$$$$$
Stop crooks,
Government needs warrant

Basic Privacy

$
Stop random strangers
HTTPS, Encrypted WiFi

https://www.tbray.org/ongoing/When/201x/2014/05/26/Privacy-Levels

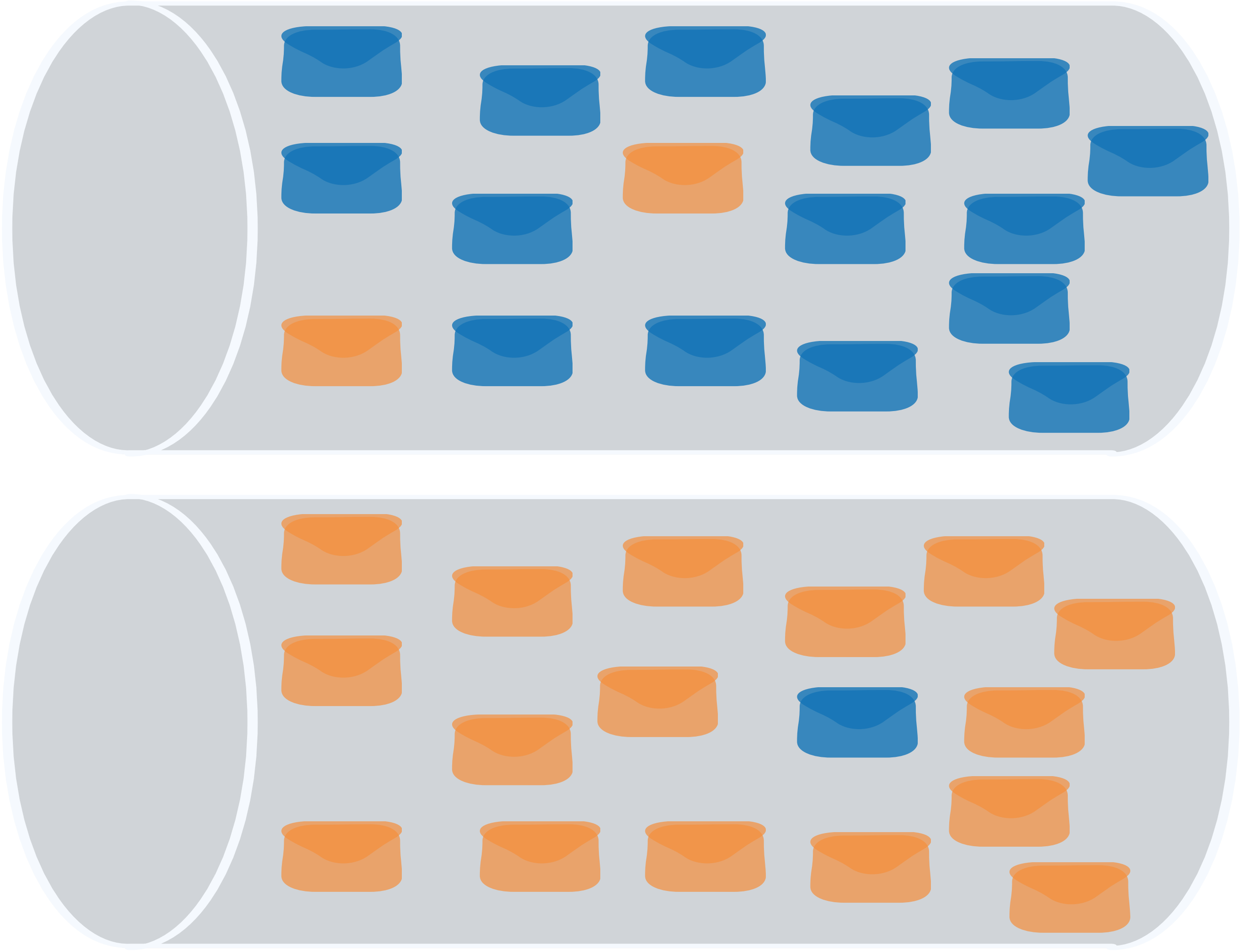


Do not
disturb

“I have nothing to hide ”

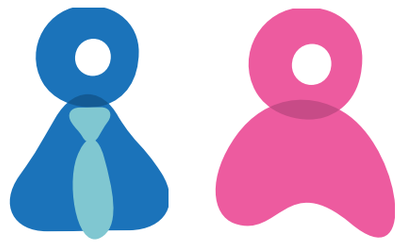
“ Nobody is interested in watching me ”

http://martinfowler.com/articles/bothersome-privacy.html



Free Society $\Rightarrow$ **Free Association and Communication**

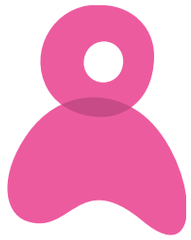
society and
the users



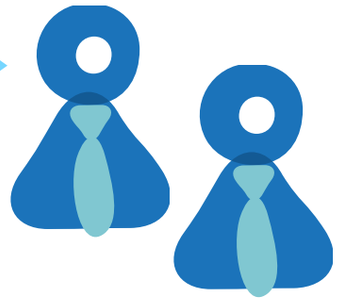
the creators
of software

– STEP 1 –

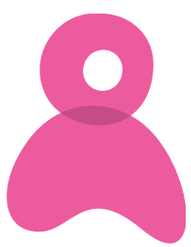
Let's build an email solution...



Maximize shareholder value!

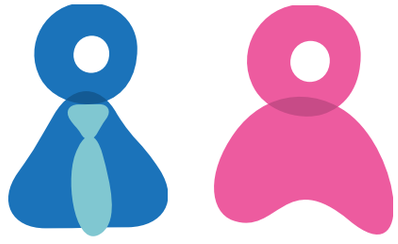


We think we found a way to make money with an email solution...

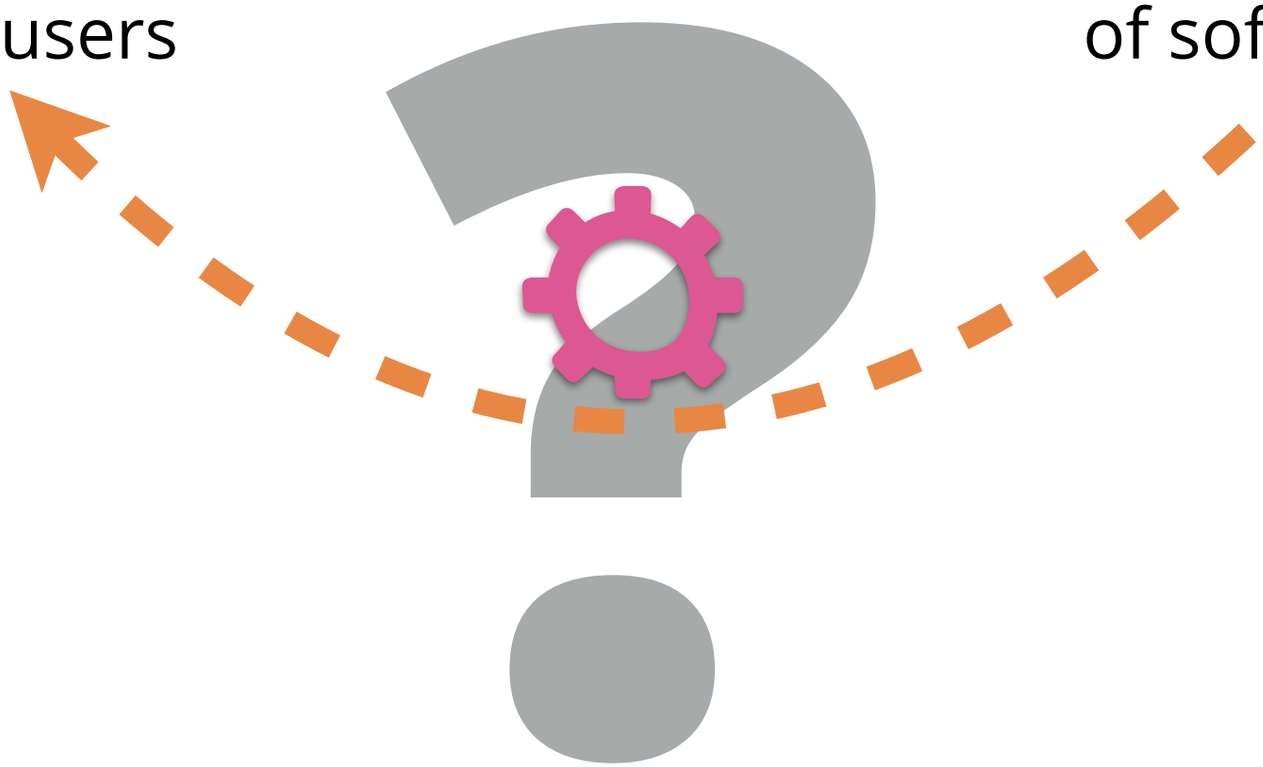


Let's build an email solution...

society and
the users



the creators
of software



Someone else is going to do it…

This is not our target group

Free markets…

blah…
blah…

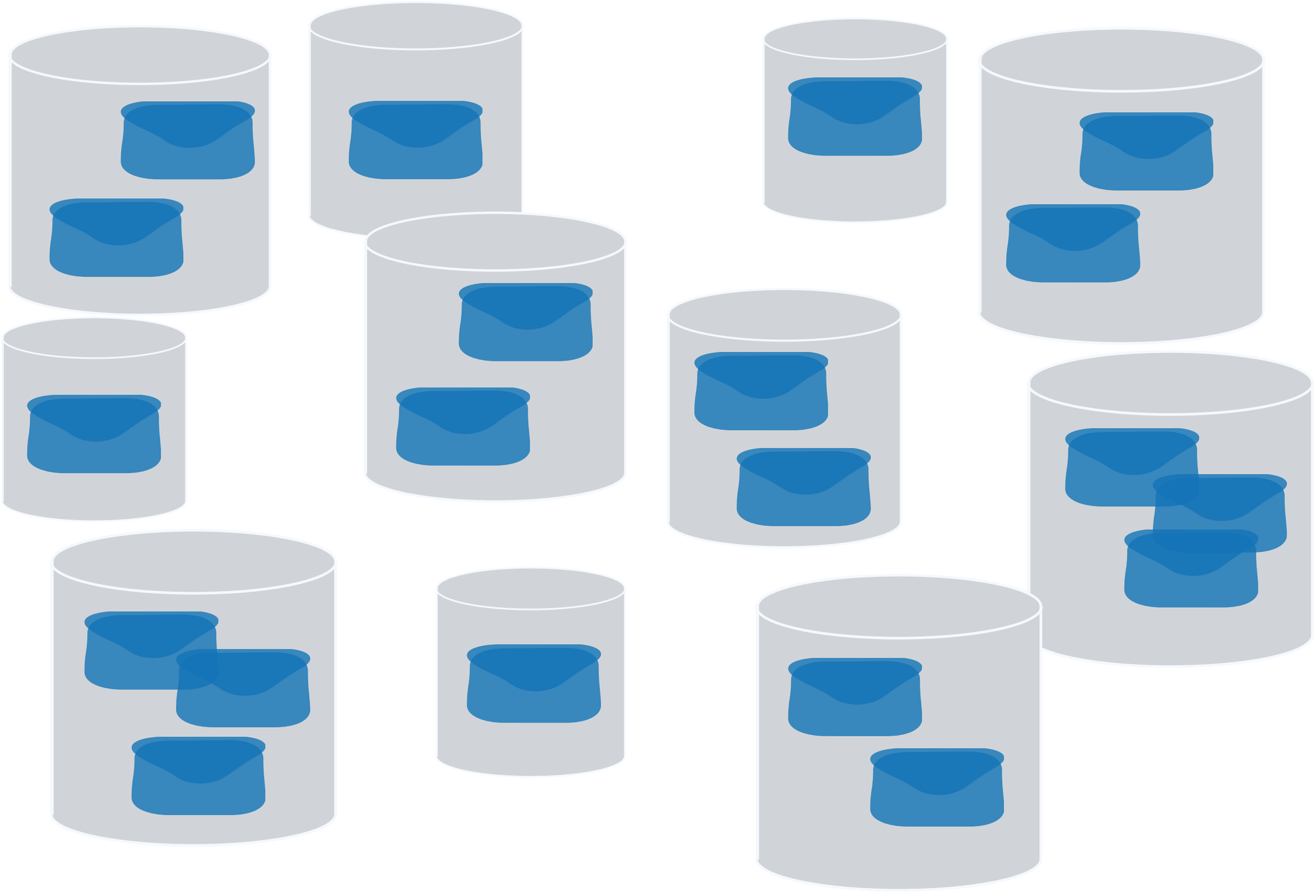
collaboration

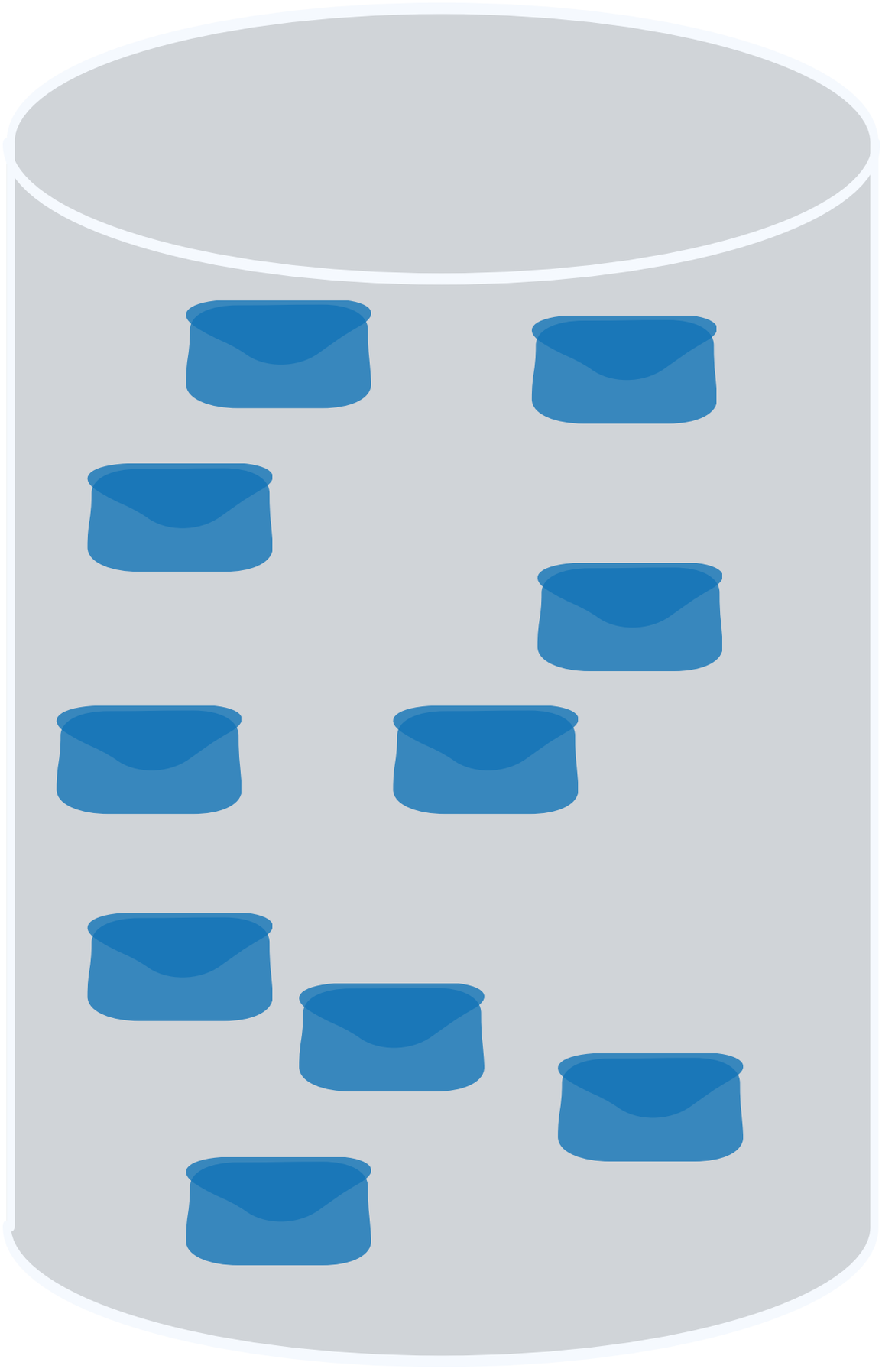
Open Source Software

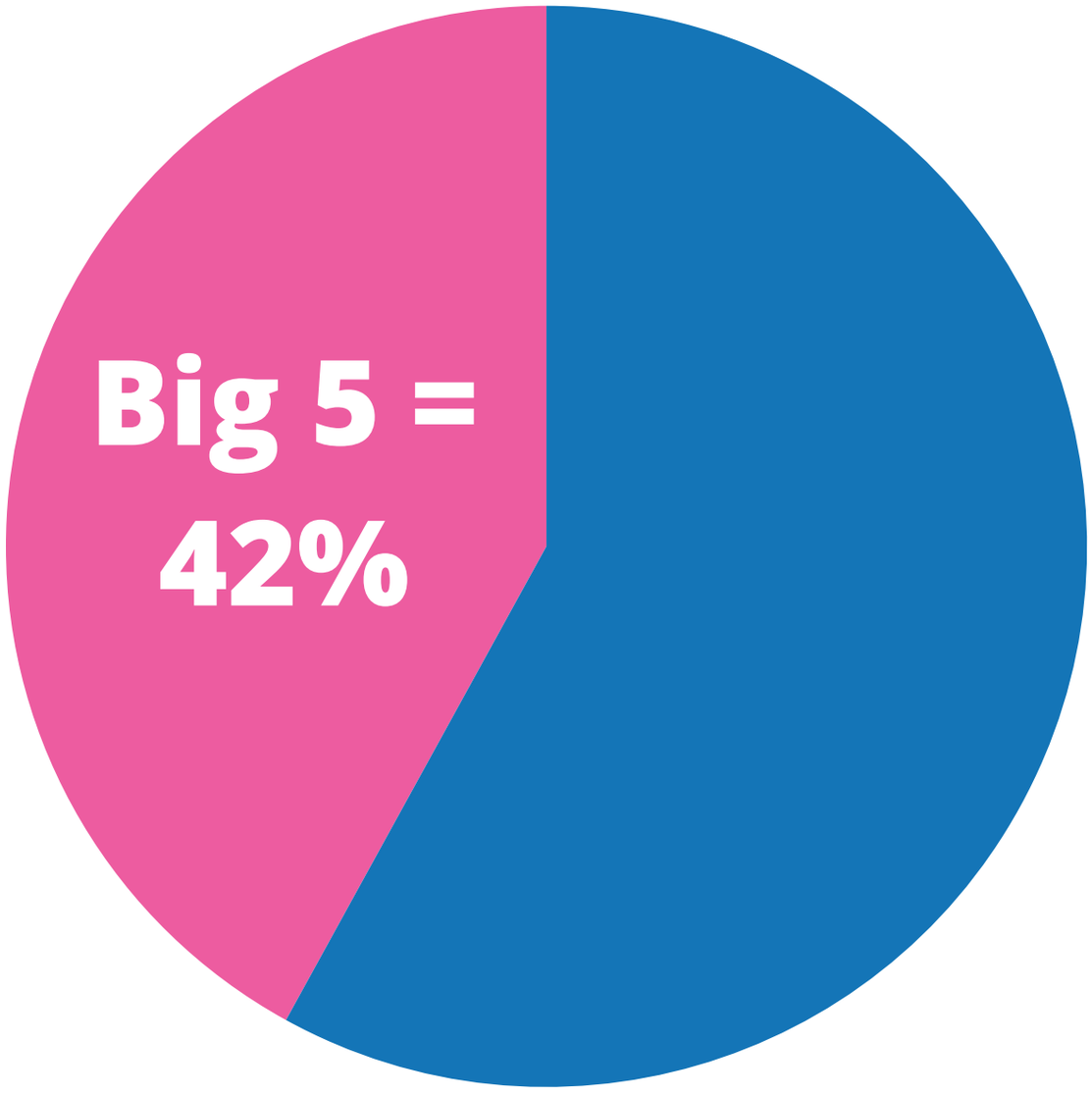
Proprietary Software

Plug-ins

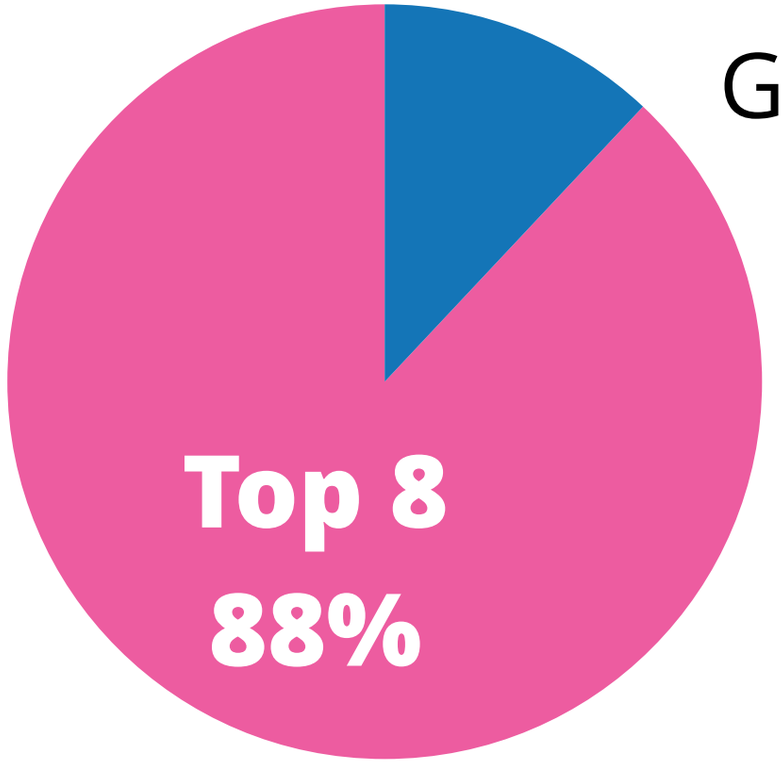
SaaS / Webmail



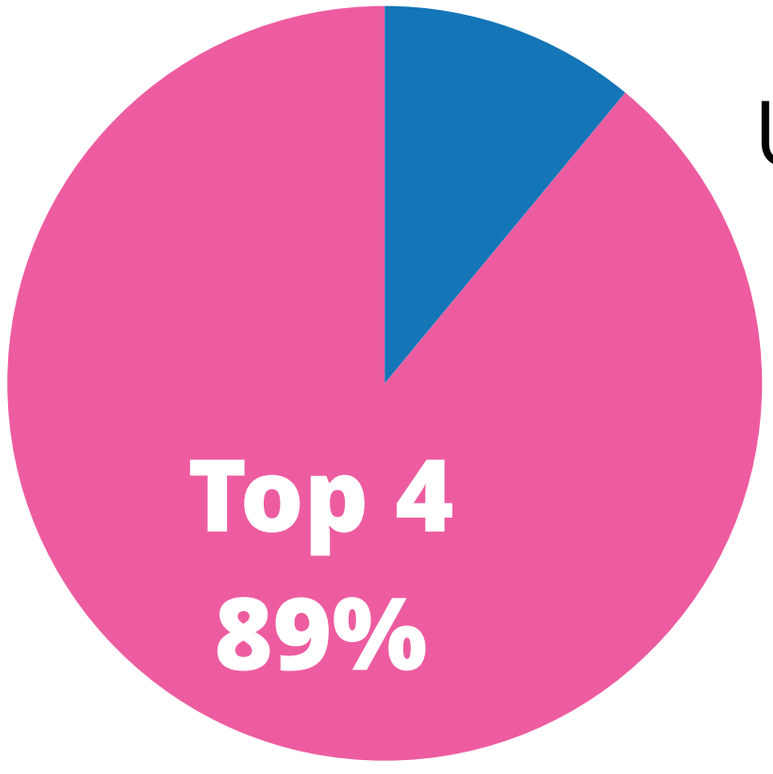




market share of the "big 5" email providers globally



Germany



USA

Judge may hold Microsoft in contempt after refusal to hand over foreign data

Obama administration contends that company with operations in US must comply with warrants for data, even if stored abroad

Share 94
Tweet 255
+1 27
Share 82
Email

Rory Carroll in Los Angeles
Follow @rorycarroll72 Follow @GuardianUS

theguardian.com, Wednesday 3 September 2014 20.08 BST

Jump to comments (100)

Technology
Microsoft · Data protection · Email · Internet

World news
Obama administration · California · Ireland · United States

More news

No matter the specific techniques involved, historically mass surveillance has had several constant attributes. Initially, it is always the country's dissidents and marginalised who bear the brunt of the surveillance, leading those who support the government or are merely apathetic to mistakenly believe they are immune. And history shows that the mere existence of a mass surveillance apparatus, regardless of how it is used, is in itself sufficient to stifle dissent. A citizenry that is aware of always being watched quickly becomes a compliant and fearful one.

~ Glenn Greenwald, No Place to Hide

opaque pricing

Jeremy Hammond

Stratfor | Geopolitical intel...

www.stratfor.com

STRATFOR
GLOBAL INTELLIGENCE

Search Stratfor.com

Analysis | Topics | Regions | Forecasts | Free | Maps & Videos | About Us

SEP 25, 2014 | 09:53 GMT

U.S.-Led Airstrikes Continue to Degrade Islamic State, Other Militant Groups

Airstrikes Sept. 24 targeted Islamic State's ability to generate funds and conduct offensives, although a shift in tactics has allowed the militants to mitigate some of the damage.

GEOPOLITICAL DIARY »

China Stays the Course as Housing Woes Intensify

Beijing continues to eschew nationwide measures to support the real estate sector, relying instead on local government interventions.

SEP 24, 2014 | 20:55 GMT

EDITOR'S CHOICE

Obama's Islamic State Strategy: Intel, Advisers and No Boots on the Ground

GEOPOLITICAL WEEKLY »

By George Friedman

Centripetal and Centrifugal Forces at Work in the Nation-State

SEP 23, 2014 | 03:00 GMT

GLOBAL AFFAIRS »

By Robert D. Kaplan

Nile Water Wars?

SEP 24, 2014 | 03:02 GMT

SECURITY WEEKLY »

The Jihadist Kidnapping Th

SEP 25, 2014 | 03:00 GMT

From: Anya Alfano
To: burton@stratfor.com, scott.stewart@stratfor.com, bart.mongoven@stratfor.com, burtonfb@att.blackberry.net

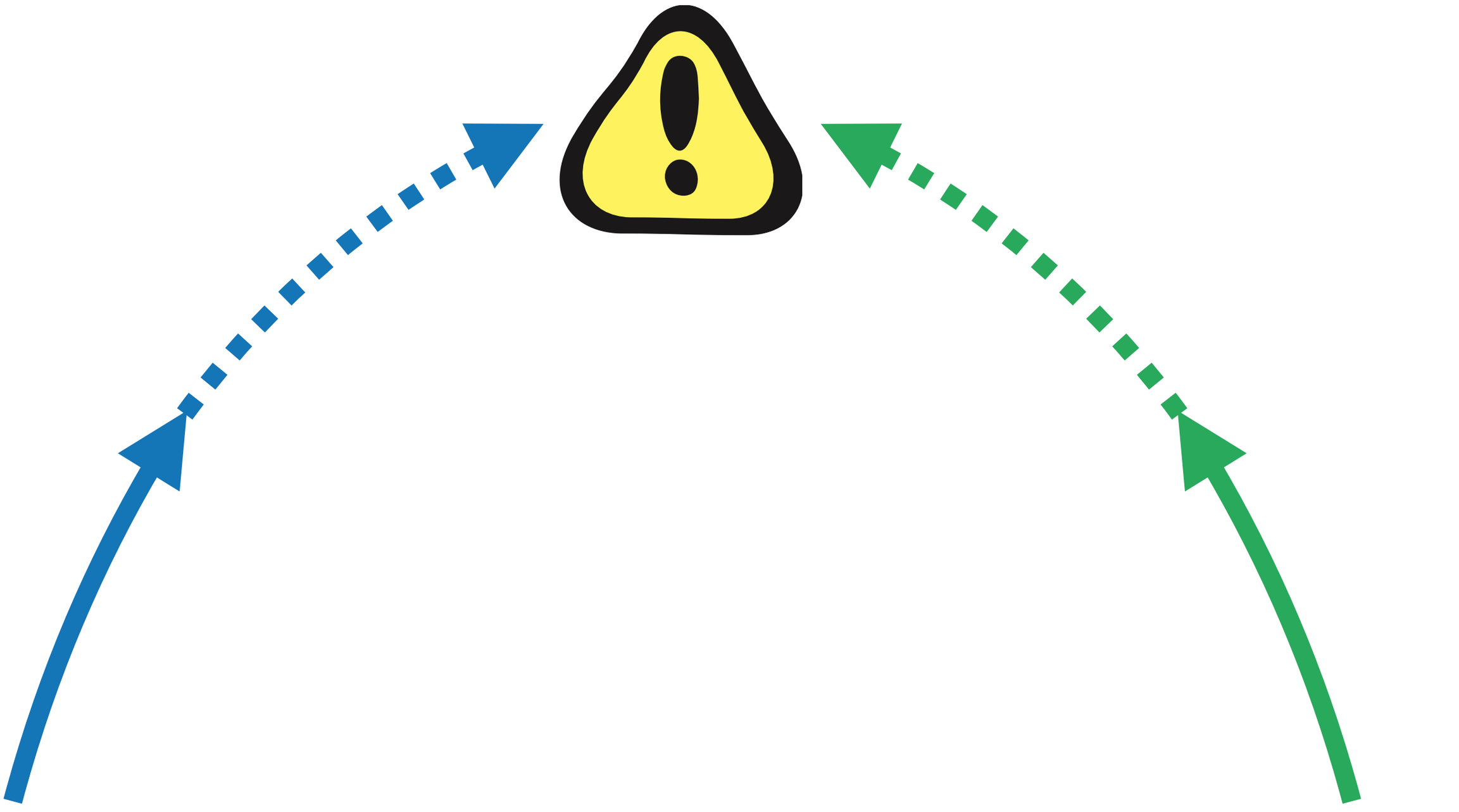
Interesting, thanks Fred.

Fred Burton wrote:

The FBI has a classified investigation on PETA operatives. I'll see what I can uncover.

Sent via BlackBerry by AT&T

Is your home in need of a little cache? This classy kitten will be happy to oblige.
READ MORE>
Sign Up to see what your friends like.
Follow @peta 518K followers +1 10 K+
http://wikileaks.org/gifiles/docs/52/5282628_re-public-policy-question-for-coca-cola-.html
Filthy N.C. Dairy Farm Shuts Down Following PETA Investigation



opaque pricing

seeping of protected data
into the commercial sector

PIXELATED

https://github.com/pixelated-project

PRINCIPLES FOR PIXELATED

We aim for mass adoption

Although we care about individuals that are targeted and need special protection, we can't do enough to help them directly (yet).

We write Open Source Software

And will endeavour to make sure the code remain open, free and libre.

We deliver a software product

And will leave to others to provide services based on it.

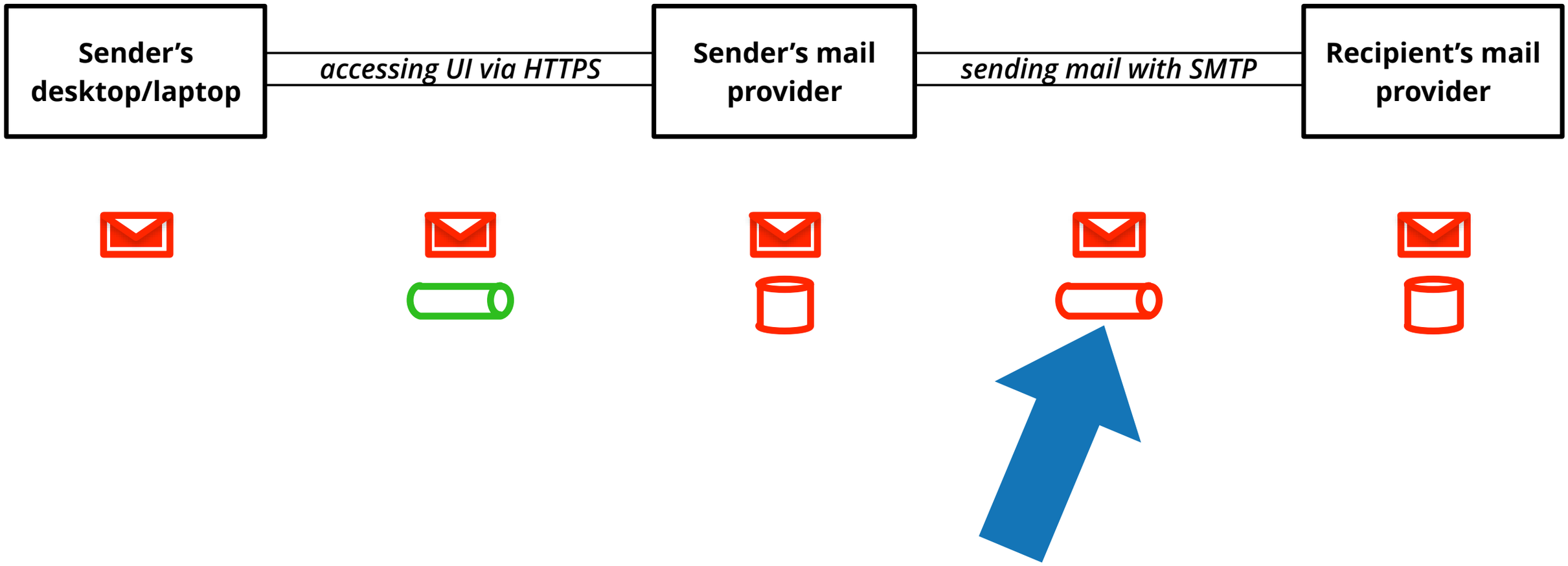
We work in the context of the *broken internet*

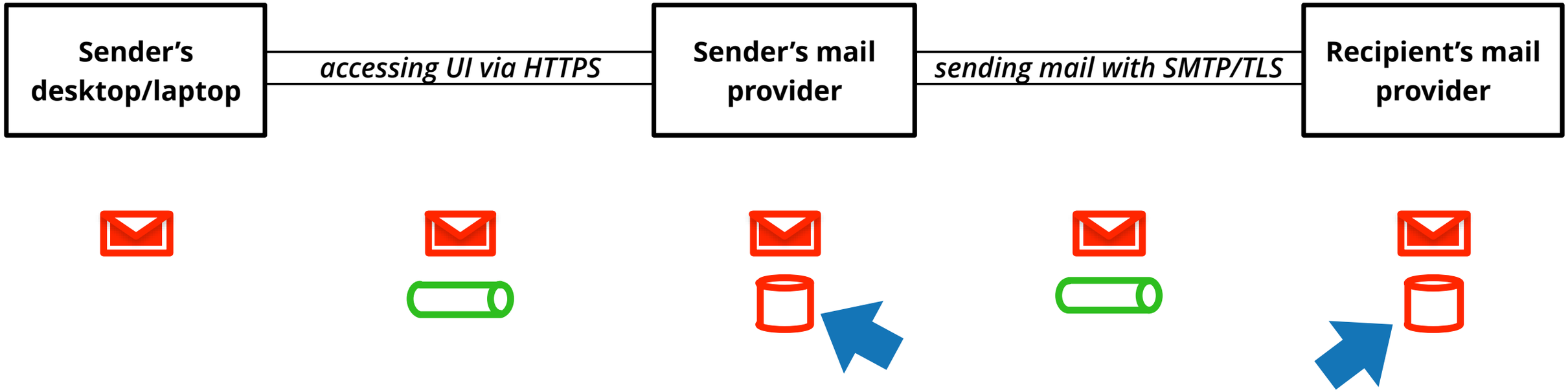
Accepting that some of its infrastructure is fundamentally flawed.

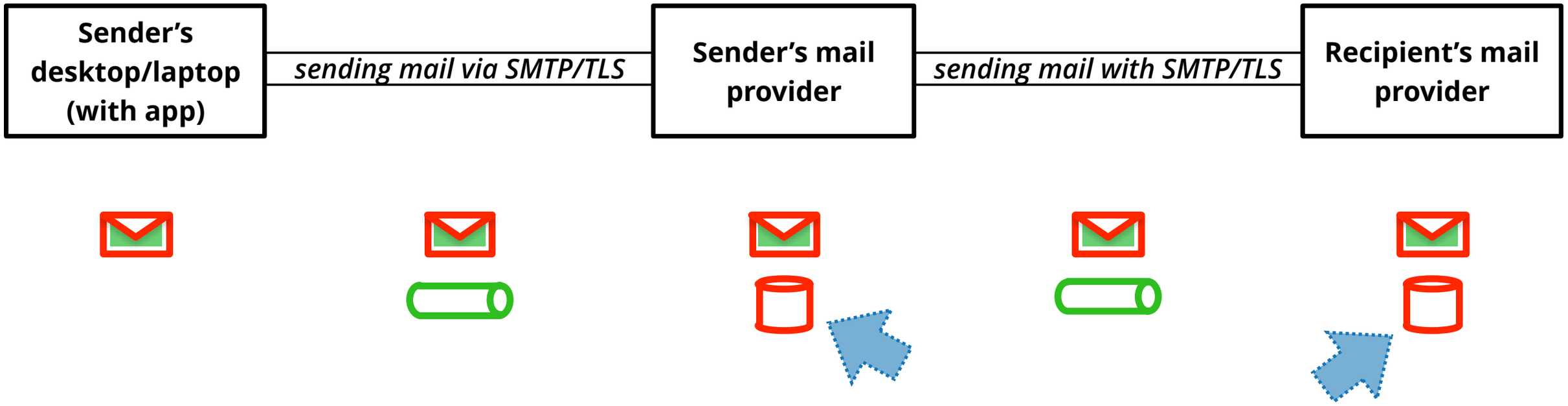
crypto

UX

+ license

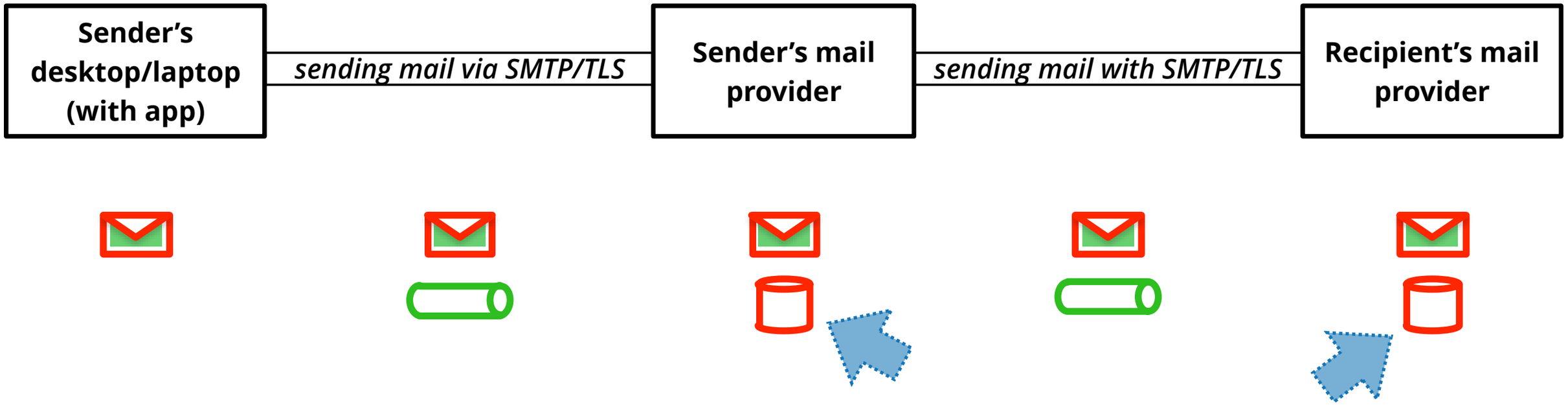

Sender's desktop/laptop
accessing UI via HTTPS
Sender's mail provider
sending mail with SMTP
Recipient's mail provider

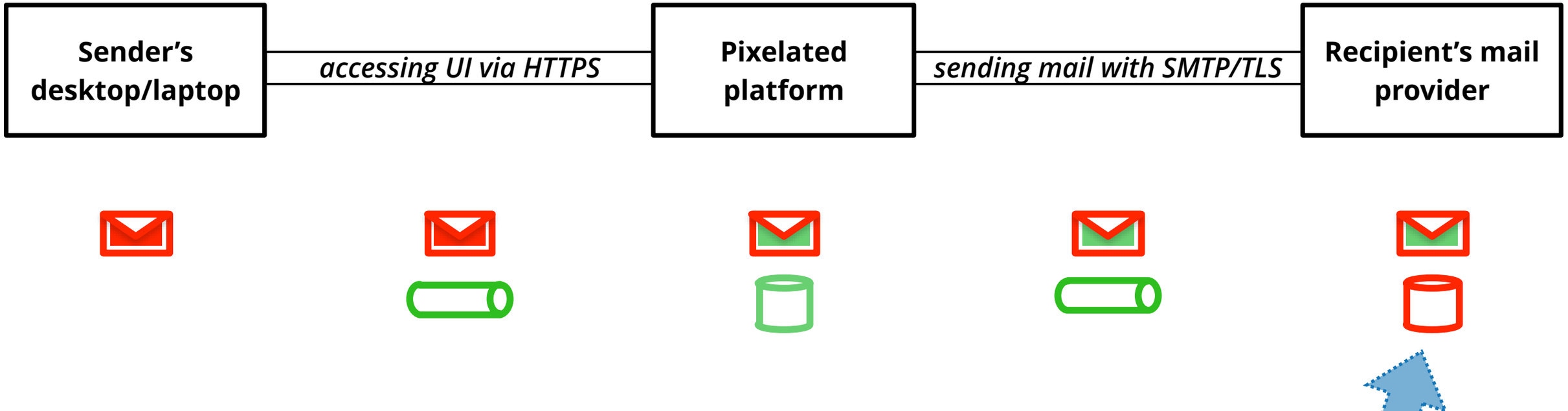

Sender's desktop/laptop
accessing UI via HTTPS
Sender's mail provider
sending mail with SMTP/TLS
Recipient's mail provider

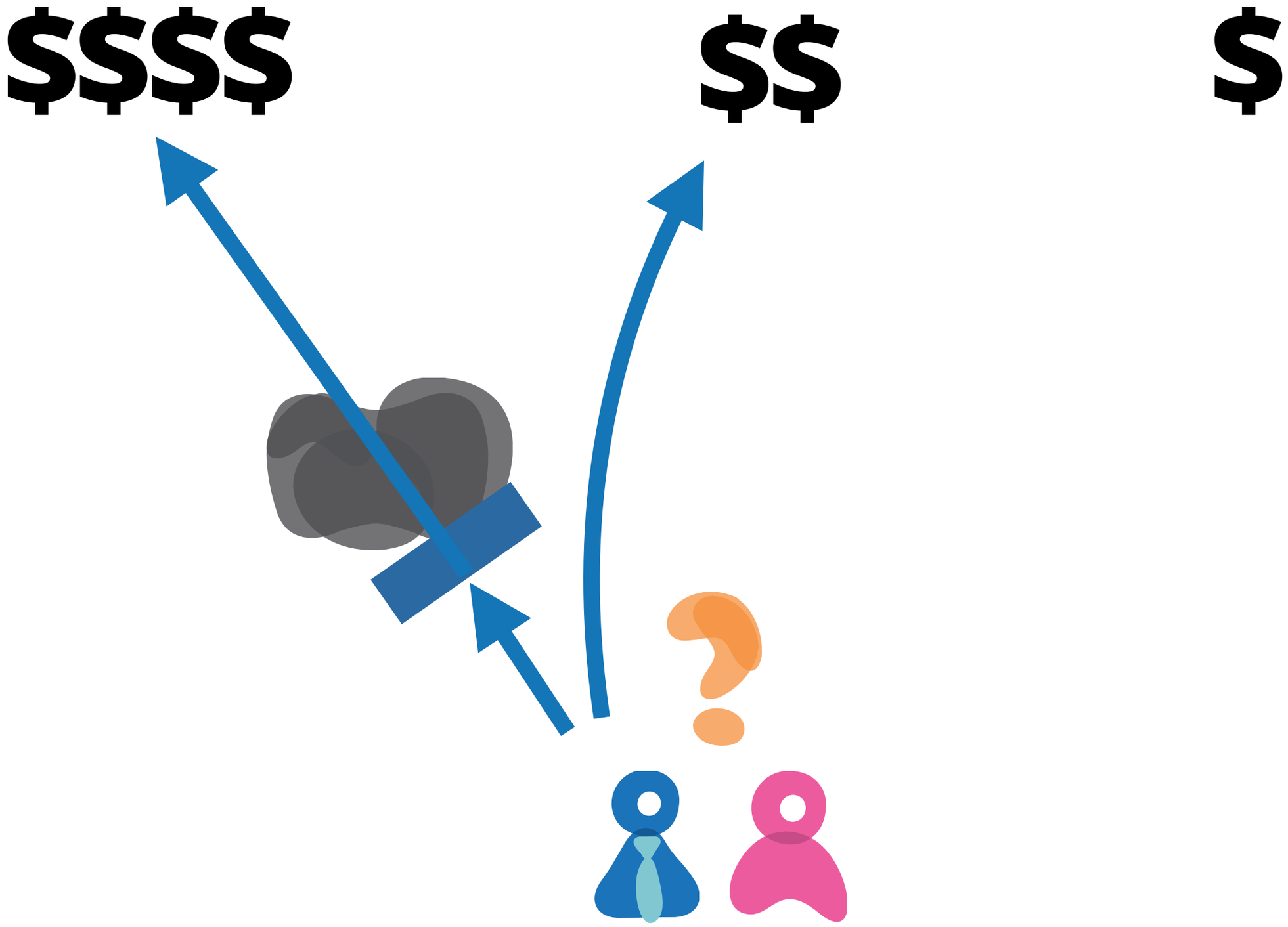

Sender's desktop/laptop (with app)
sending mail via SMTP/TLS
Sender's mail provider
sending mail with SMTP/TLS
Recipient's mail provider

```
Return-Path: <azul@blue.net>
Delivered-To: lalala-erik@green.org
Received: (qmail 15178 invoked from network); 26 Feb 2014 20:21:02 -00
Received: from unknown (HELO mx1.blue.net) (123.456.123.456)
  by host.green.org with SMTP; 26 Feb 2014 20:21:02 -0000
Received: from somehost.blue.net (somehost-c.blue.net [10.0.1.75])
  (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
  (Client CN "*.blue.net", Issuer "Gandi Standard SSL CA" (not verifie
  by mx1.blue.net (Postfix) with ESMTPS id F2B9F514C9
  for <erik@green.org>; Wed, 26 Feb 2014 12:20:51 -0800 (PST)
Received: from [127.0.0.1] (localhost [127.0.0.1])
  (Authenticated sender: azul@somehost.blue.net)
  with ESMTPSA id BF16616F
Message-ID: <530E4C95.8070009@blue.net>
Date: Wed, 26 Feb 2014 21:20:37 +0100
From: azul <azul@blue.net>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20100101
Thunderbird/24.3.0
MIME-Version: 1.0
To: erik@green.org
Subject: Meeting next week in Berlin
X-Enigmail-Version: 1.5.2
Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="d5JFglPwD2tqiMaWvFgKk5Cs3F1PdmJiR"
X-Virus-Scanned: clamav-milter 0.97.8 at mx1
X-Virus-Status: Clean
```

```
This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)
--d5JFglPwD2tqiMaWvFgKk5Cs3F1PdmJiR
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--d5JFglPwD2tqiMaWvFgKk5Cs3F1PdmJiR
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.14 (GNU/Linux)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

hQEMA3Ro3A0DaxBgAQgAjzi0HFlycY6PwDxO4W+CS08W3hxvvrynwab58k8enEAk
tpXroDwA6CXHz5fAvmPgSSxCHyC5QzL9GGUtJhHQGzyom4nab4f0ZCIkdoG22IZj
uyUCp/XdcQCNvi6dkjgd9wveL7NeGD2b7DThHFE0VyE1DWyNyYUH3RgEIk3STMO3
4K0KIPJHN+6/yP5NJDMAmIK/hj0BV/q9ExnyLNSO77tisWxCsJWu/LNvoiXQOg19
4LWBVMUHuMiMZ3W6b2bMwcoToDxwct1JJFbXRGuk0N69Wi26tk9eHji82Kb00Dme
WGM1UtDpP9trFuisMM9GcqZ0uEL8YfW/eJs4mpNF1IUCDAPkhsUENPcWWwEP/AoB
/RtXIMAml6AQOVyhWJDSeK8kRD/o/mtXFLZuFWxJ8ry8b3pbYCVheQQbvg34dmJ0
QCipBZYyUkS25eY9wwRWenVQ+H1cZLk/6uElA781zynYK3CDHi5qc7+tuLyuhlgx
baCAtktiH9e6p4qSCvZVQq83Rtg6yGR7Lfe4TLGa4zH1kppGtxm9OvGTqvW4FrrC
W9uBKpYdNg7D0yO60XHxk6KZOIEXKBd/vKEEweUYKbu64a9XZg9hGYW1thGPIUwM
```


Sender's desktop/laptop (with app)
sending mail via SMTP/TLS
Sender's mail provider
sending mail with SMTP/TLS
Recipient's mail provider


Sender's desktop/laptop
accessing UI via HTTPS
Pixelated platform
sending mail with SMTP/TLS
Recipient's mail provider



BEING RESPONSIBLE

over

MAXIMISING GAIN