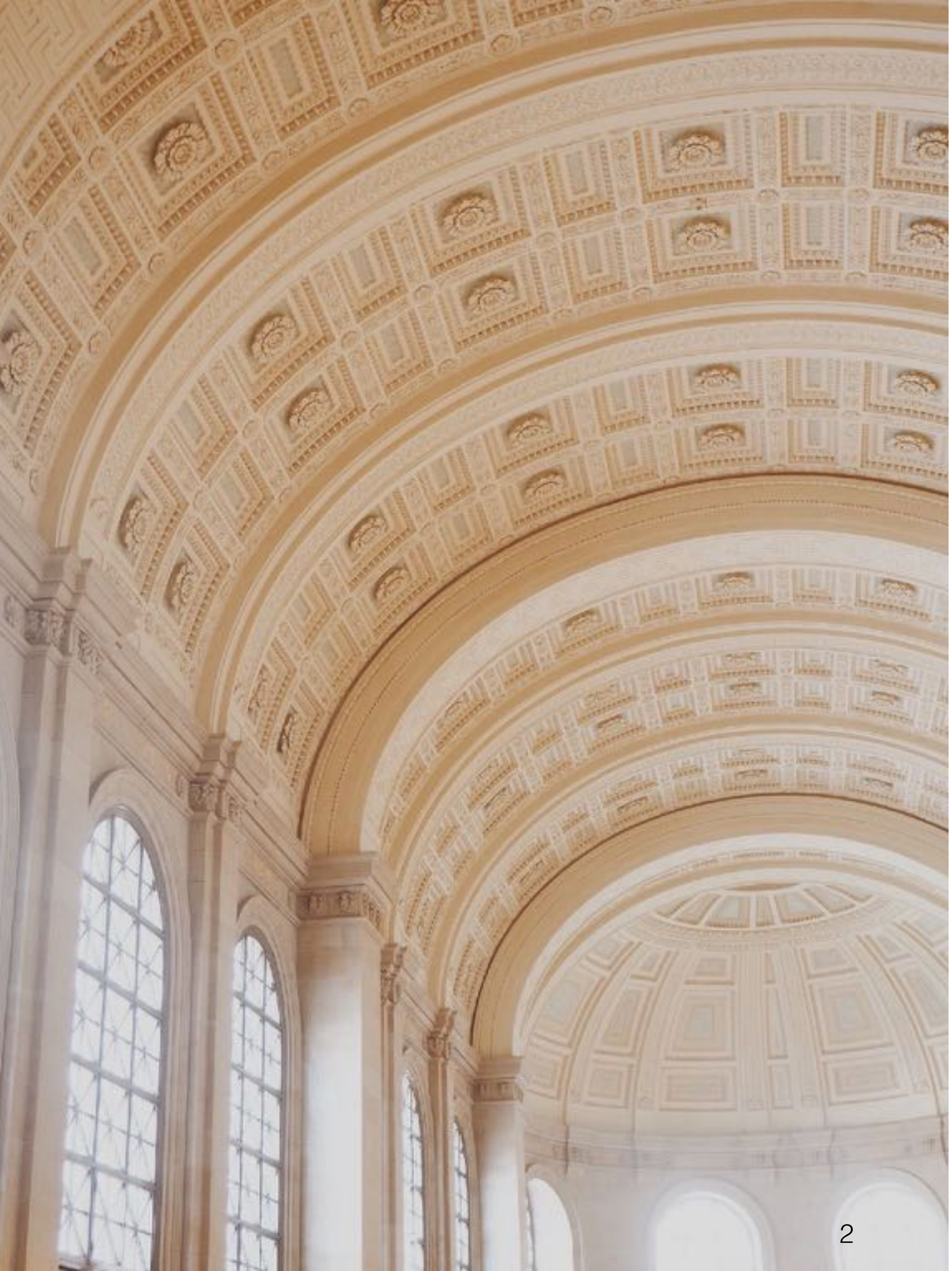
DNS Privacy Interest and Concerns

RIPE 76
May 2018

Vicky Risk
ISC.org
vicky@isc.org

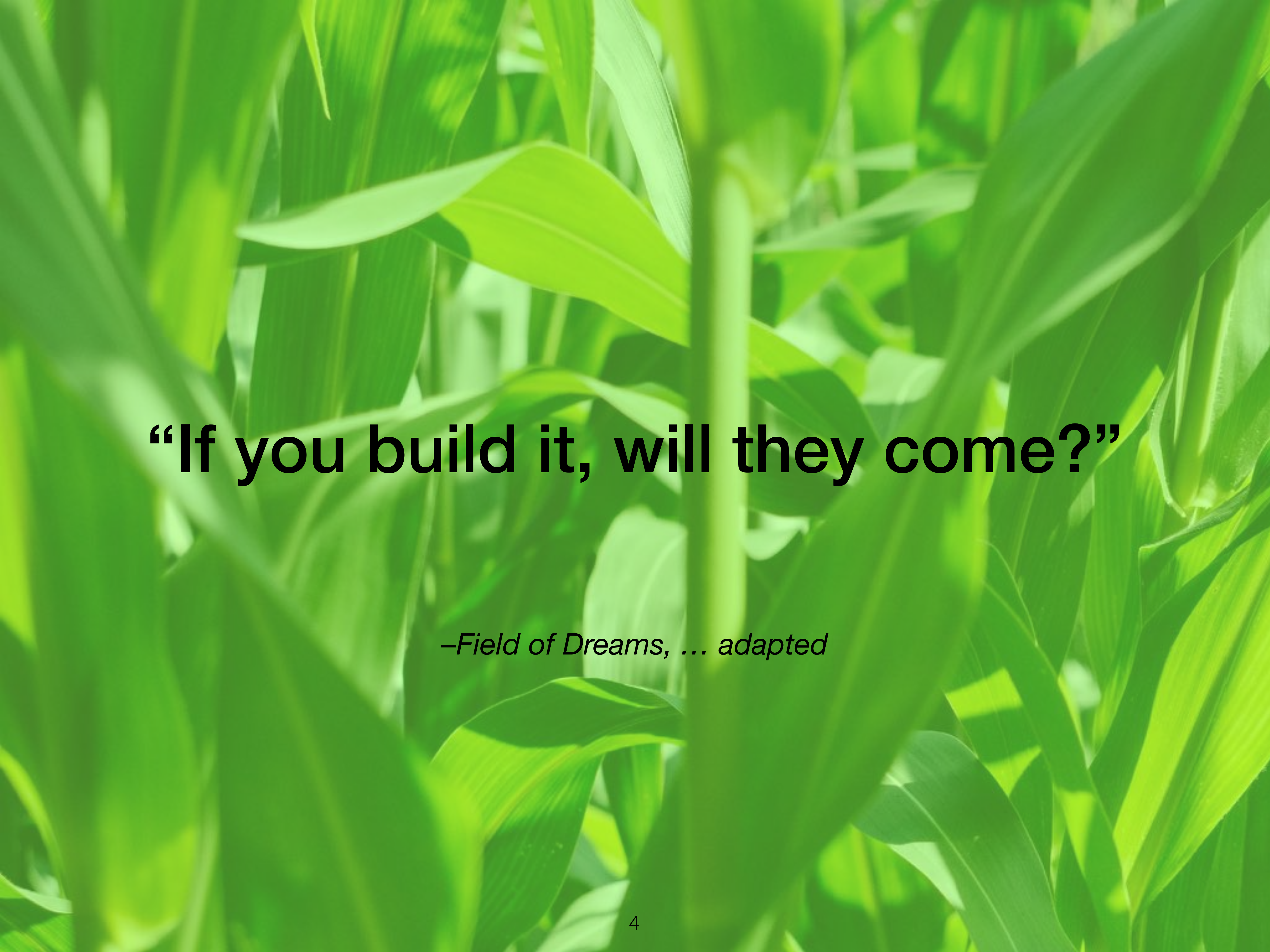


IETF Community

- Pervasive monitoring is an attack
- The Internet has turned into a surveillance tool
- Internet users have a right to privacy
- Must fix!!!!

Operators concerns

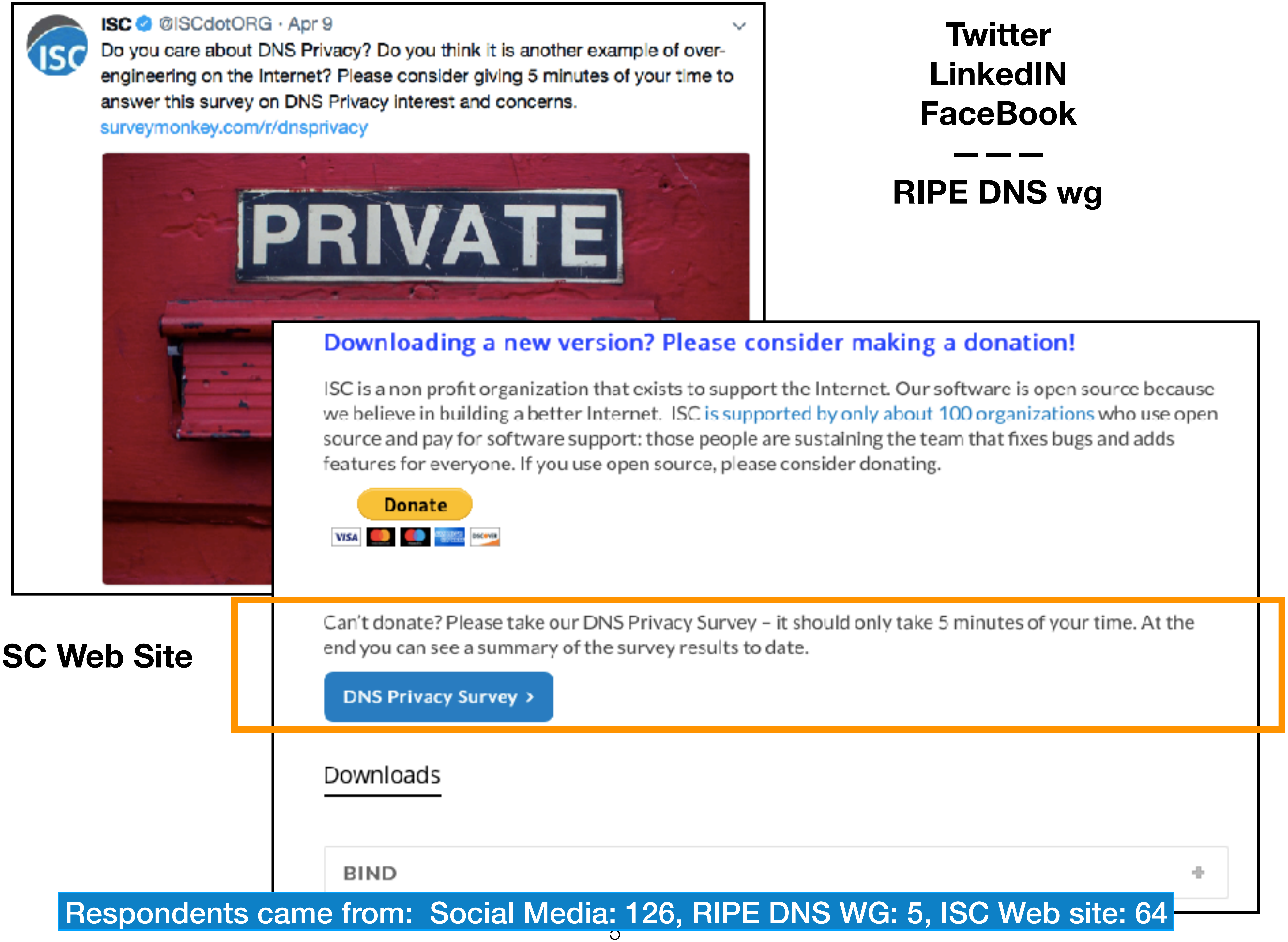
- User demand?
- Business benefit?
- Operational overhead?
- Is this an important problem?



“If you build it, will they come?”

–Field of Dreams, … adapted

Survey open March 27 - May 4, 2018



ISC @ISCdotORG · Apr 9

Do you care about DNS Privacy? Do you think it is another example of over-engineering on the Internet? Please consider giving 5 minutes of your time to answer this survey on DNS Privacy interest and concerns. surveymonkey.com/r/dnsprivacy

Downloading a new version? Please consider making a donation!

ISC is a non profit organization that exists to support the Internet. Our software is open source because we believe in building a better Internet. ISC is supported by only about 100 organizations who use open source and pay for software support: those people are sustaining the team that fixes bugs and adds features for everyone. If you use open source, please consider donating.

Can't donate? Please take our DNS Privacy Survey – it should only take 5 minutes of your time. At the end you can see a summary of the survey results to date.

Twitter
LinkedIN
FaceBook
— — —
RIPE DNS wg

ISC Web Site

Respondents came from: Social Media: 126, RIPE DNS WG: 5, ISC Web site: 64

Survey topics

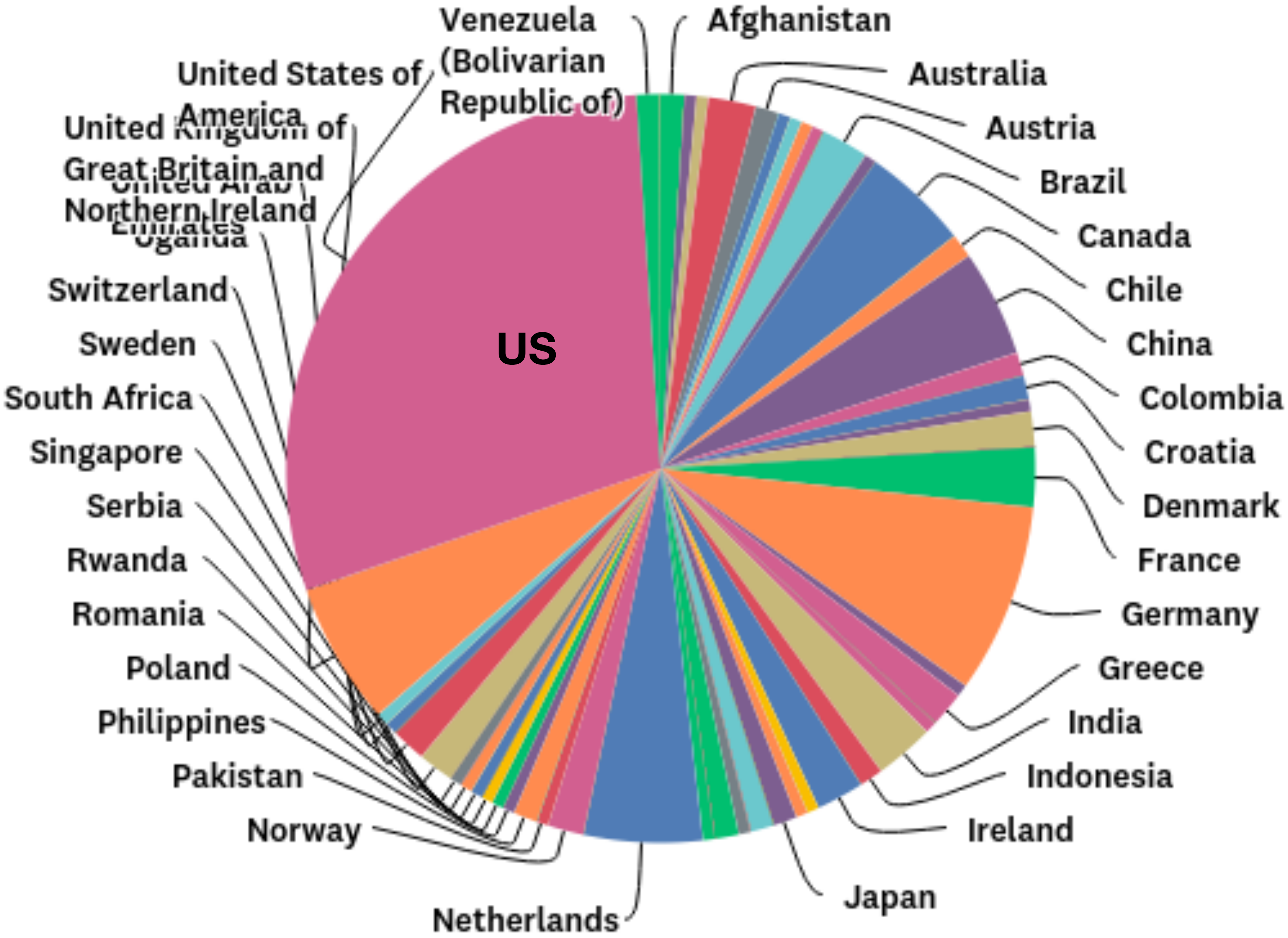
1. Demographics
2. Impact and importance of privacy on the organization
3. Deployment status of Qname minimization
4. Encryption interest and concerns
5. 9.9.9.9 / 1.1.1.1 question
6. GDPR questions

Who Responded?

Possible Privacy advocates, not necessarily representative

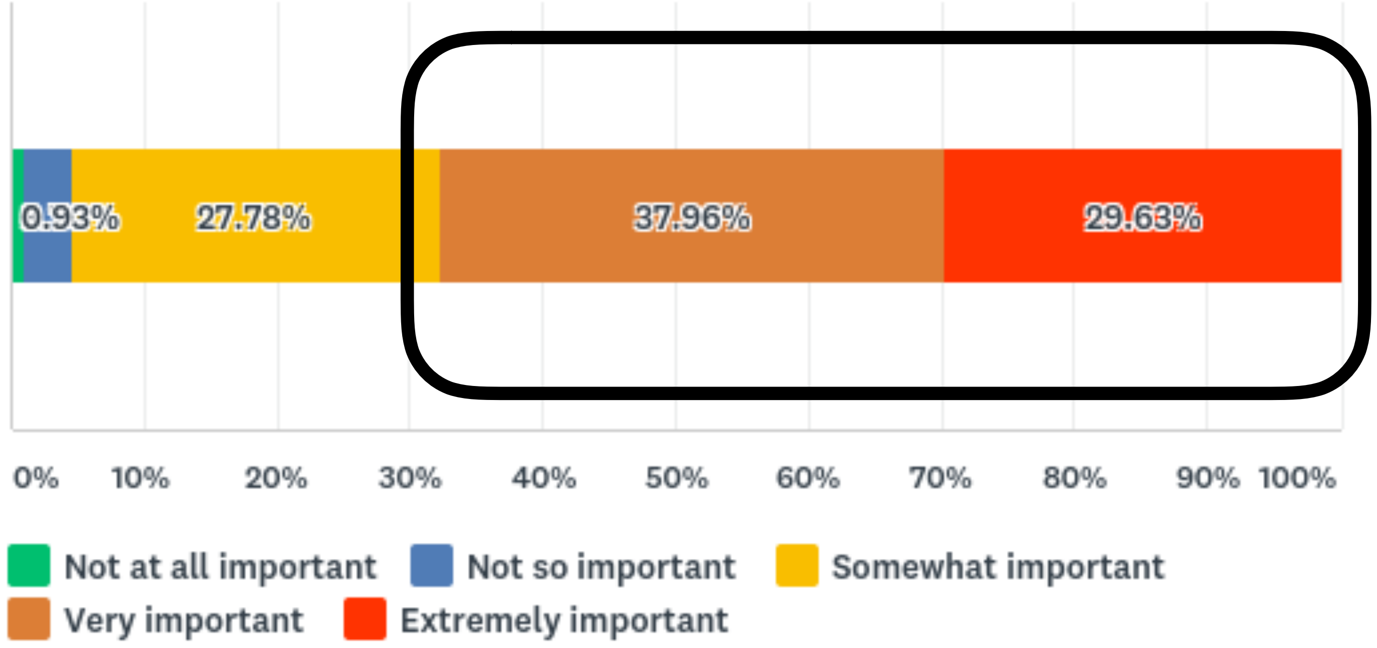
Individual consumer, Internet user	n=45	23.08%
Internet Service Provider (access + services)	n=36	18.46%
Educational organization		12.31%
In the business of creating products that leverage the Internet		10.26%
Internet-enabled business		9.23%
Enterprise (not primarily dependent on the Internet)		7.69%
Hosted (cloud) services provider		5.13%
Government office		2.56%
Other (please specify) (hobbyist, consultant, small business, registrar, internet engineer…)	n=22	11.28%

Wide geographical distribution



Importance

Q3 How important are end user privacy concerns in decisions about what products and services your company offers and how those services work?



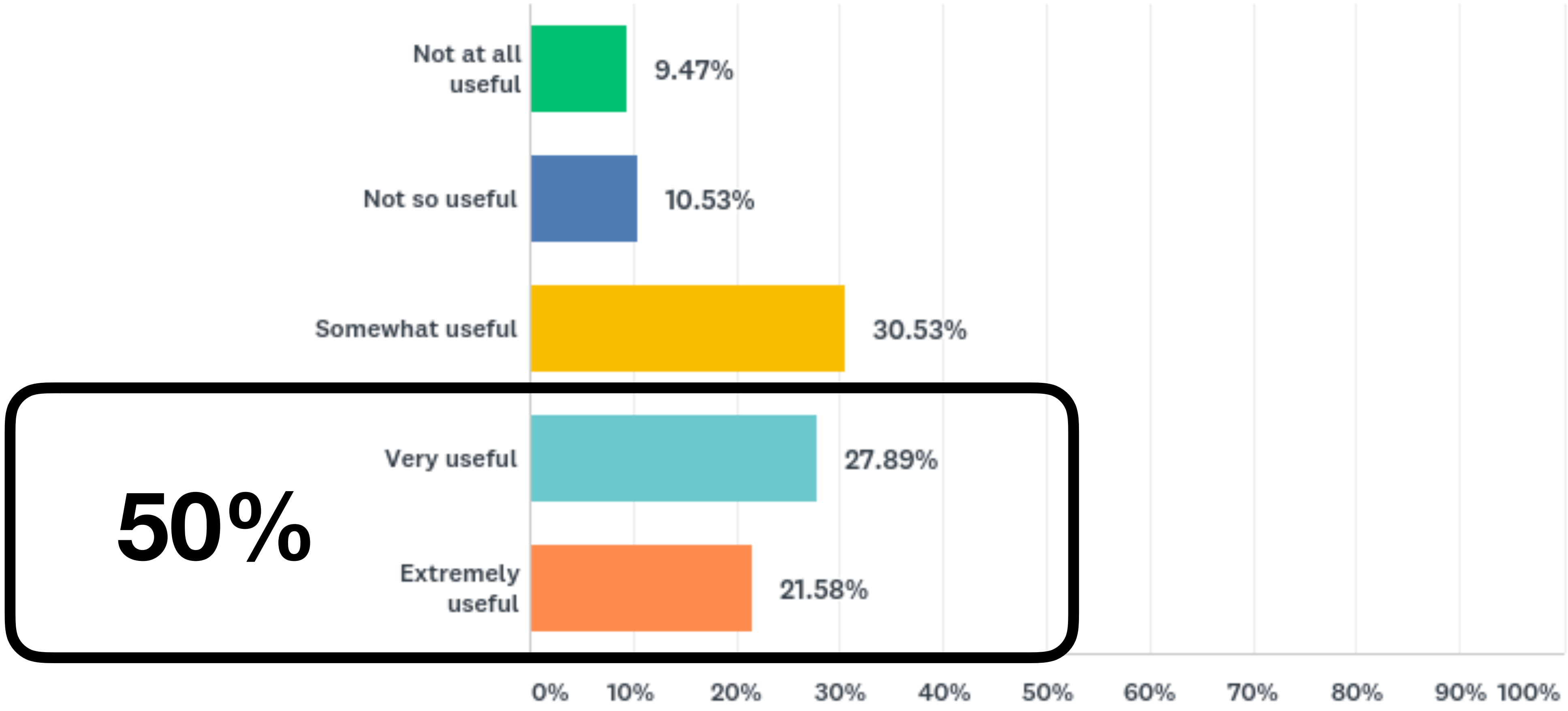
68%

excludes individuals and 'other'

Internet user data has significant marketing value

Marketing Benefit of User Privacy?

Q4 Do you see a useful marketing benefit for your company, if you can make end user privacy claims about your products or services?



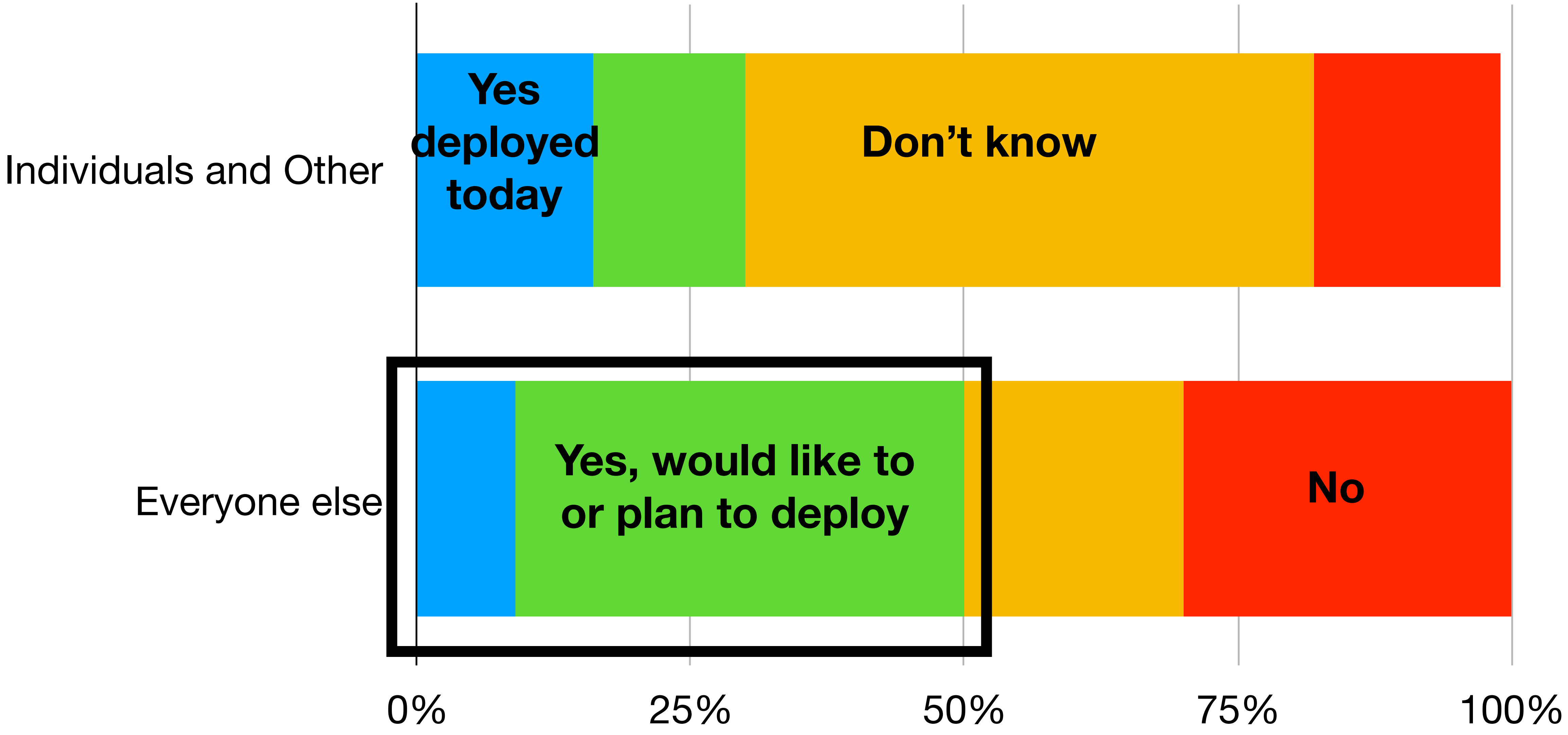
ALL respondents

QNAME question

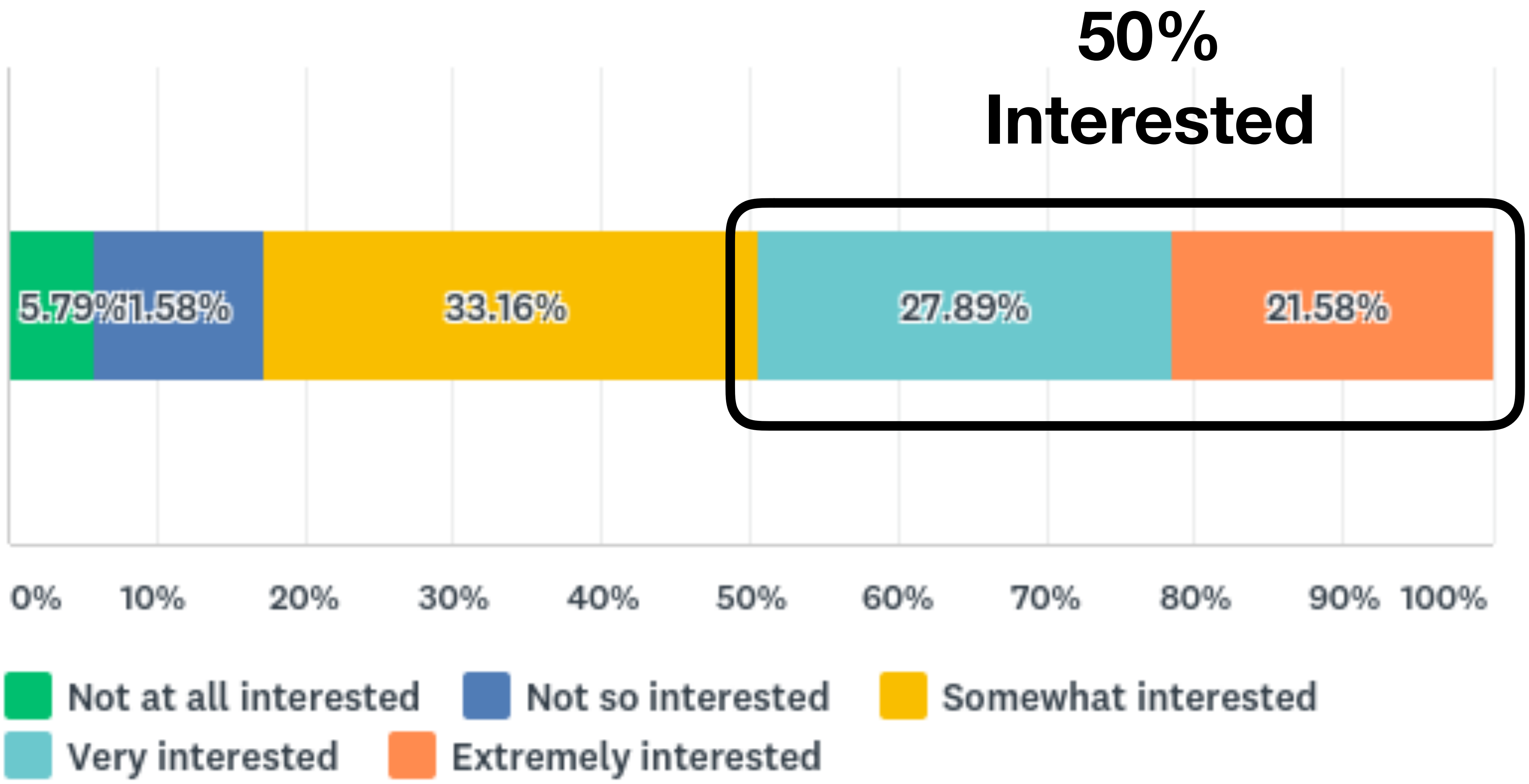
QNAME minimization minimizes the specificity of the query sent to an authoritative server to the question that authority is expected to answer.
There may be some minor side-effects, including a few non-interoperable sites, and multiple queries may be necessary to sites hosting both parent and child domains.

If this option is available, do/will you enable it?

QNAME Minimization



Interest in offering Encryption



How interested are you in offering your users the option of encrypting DNS traffic?

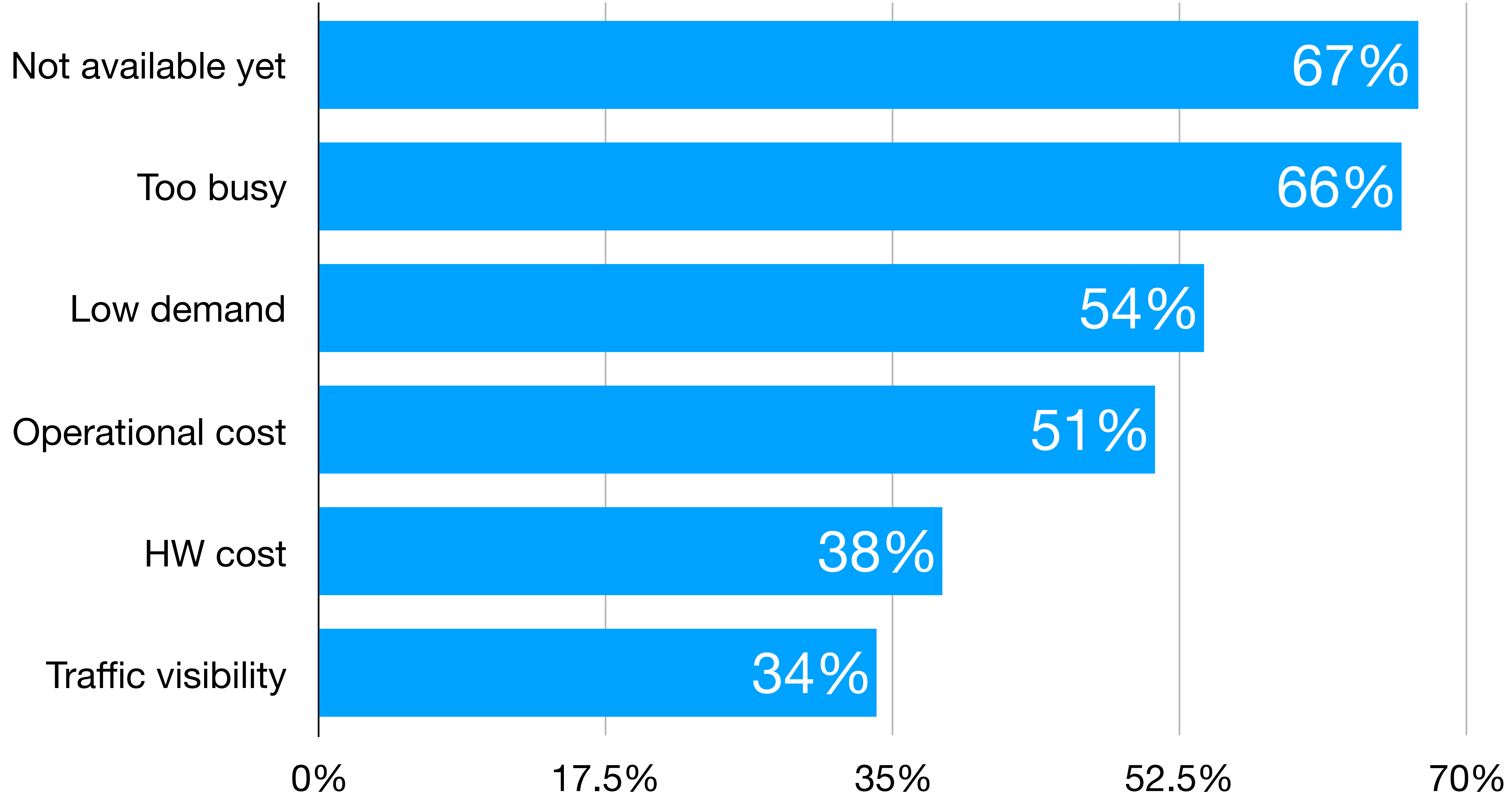
all respondents

What are the obstacles to implementing DNS Encryption?
Please rate the following factors:

- uncertain or low demand for the service
- possibility of increased hardware cost
- possibility of increased operational cost
- loss of visibility into encrypted traffic
- products or services I use currently don't support encryption
- no time or resources to develop the service

Rating Scale
Significant obstacle
Somewhat significant
Minor consideration
Not a factor

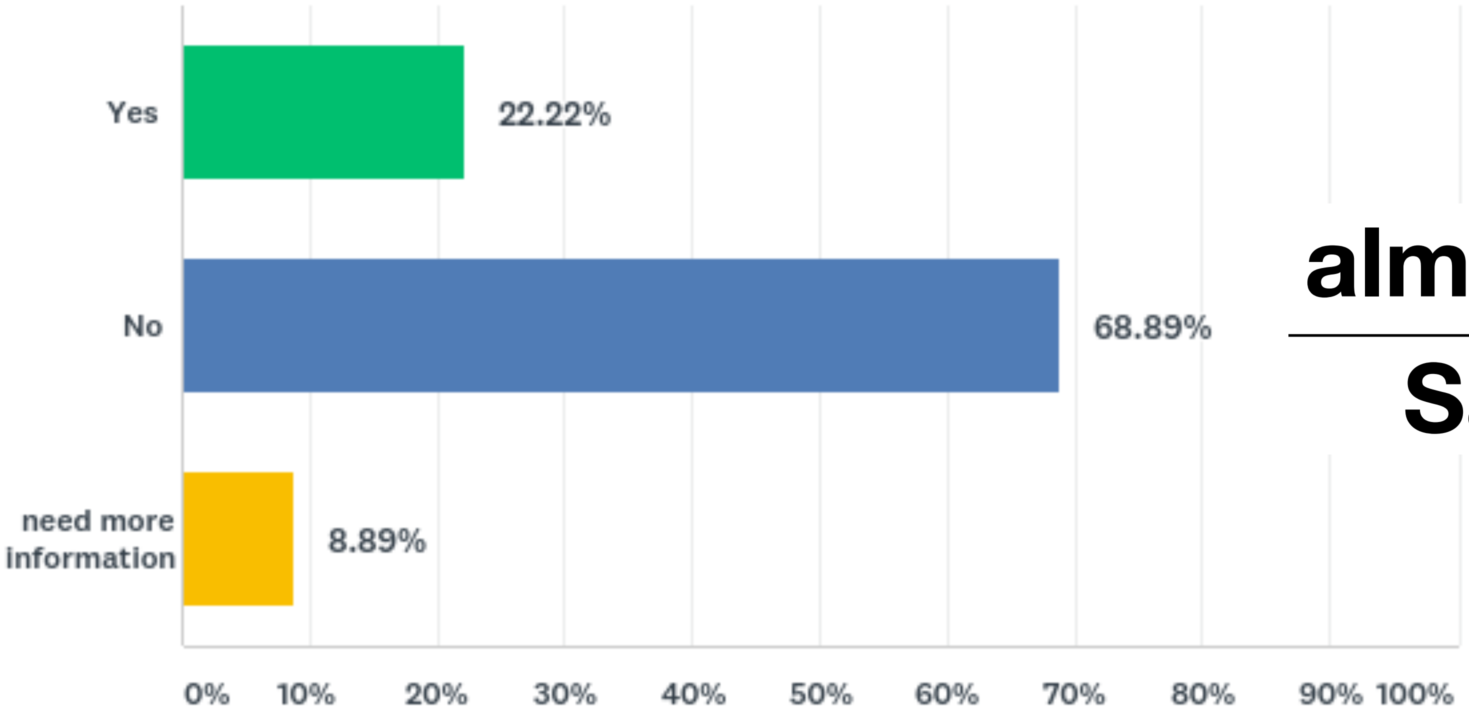
Significant obstacles to enabling encryption



top 2 ratings, excludes individuals and ‘other’

Public Hosted Service

Q9 Would you consider migrating your users to a free, public hosted DNS resolver service that implements DNS privacy features? (such as 9.9.9.9 or the recently launched 1.1.1.1)?



almost 70%

Say NO

excludes individuals and ‘other’ - who were more willing to use one of these services

Overall Summary

1. End user privacy is very important in decision-making (70%)
2. There is a useful marketing benefit in respecting privacy (50%)
3. Half plan to or have deployed QNAME minimization
4. Half are interested in offering encrypted DNS, without getting into details about how this might be done, but
5. Most reported significant obstacles to offering encryption, including lack of feature availability (which we can fix) and operator time to deploy.
6. Almost 70% are skeptical about using hosted DNS privacy services. Individuals were more open to using a hosted DNS privacy service than respondents who are supporting multiple users

Thank You

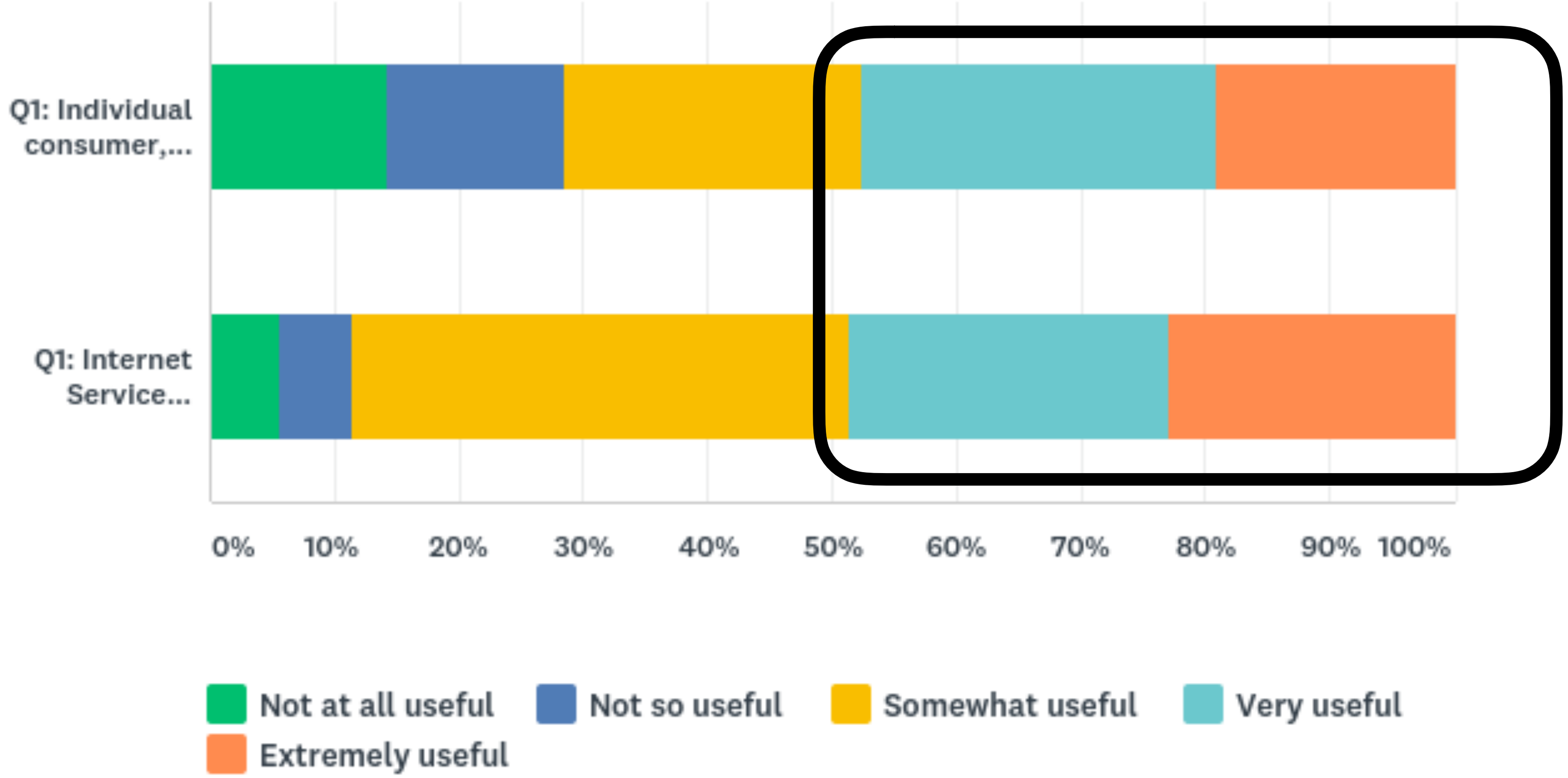
Vicky Risk, vicky@isc.org
Contact me if you would like the full dataset

What impact have privacy concerns had on your organization?

A factor in the selection of products to use on the (internal) network	57.14%
A factor in the selection of outsourced or hosted (private or hybrid cloud) services	52.57%
Additional rules and restrictions around capture and analysis of network traffic	42.86%
Additional rules around use and storage of web site visitor data	38.86%
Additional rules and restrictions on capture, analysis and usage of DNS data specifically	38.29%
Required creation of public disclosures such as a 'cookie' policy	30.86%
Additional compliance steps in ... (add comment below)	16.00%
Other (please specify) **Mentions of PCI, HIPPA**	16.00%

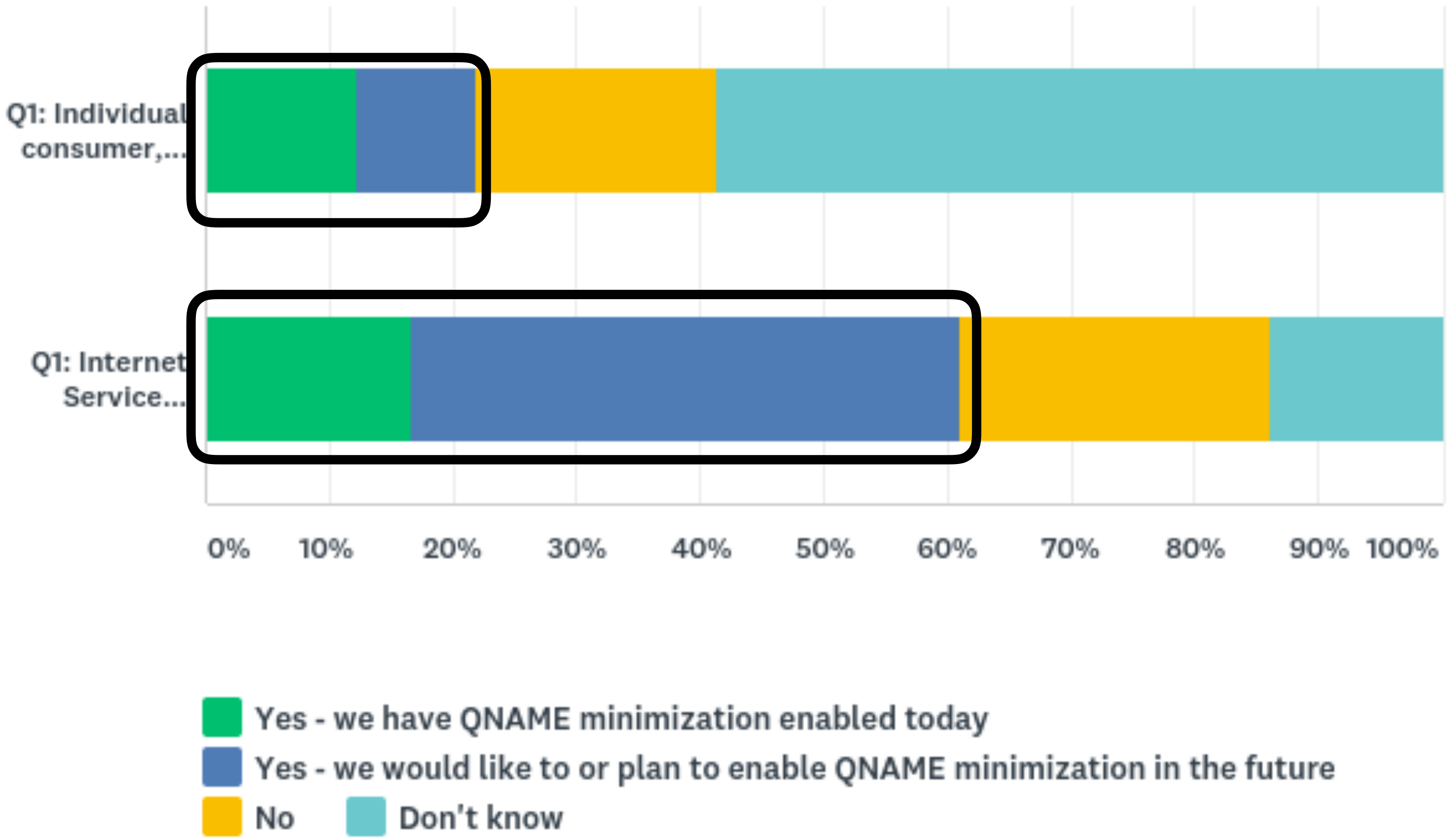
Individuals agree with ISPs

Q4 Do you see a useful marketing benefit for your company, if you can make end user privacy claims about your products or services?



comparing Individuals with Internet Service Providers

QNAME Minimization



comparing Individuals with Internet Service Providers

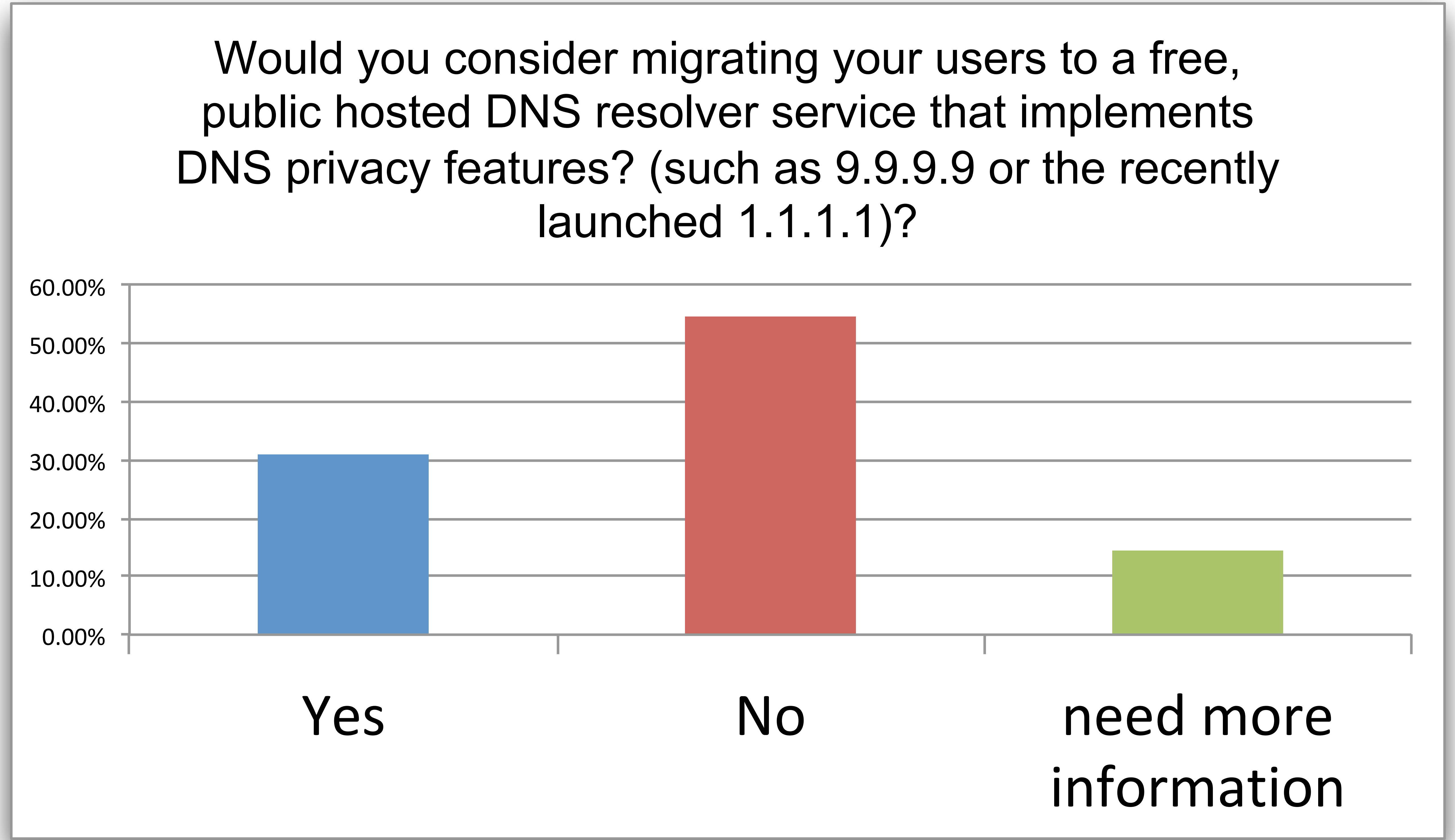
Encryption Comments

This is horribly reckless. Many things depend on query traffic, such as threat intelligence and end-user protections. In addition, there is no quantitative statement (that I am aware of) to quantitatively evaluate how much benefit this disruptive technology gives, by taking away the demonstrable benefits of DNS query analysis.

DNS encryption has to be fully implemented in future RFCs and in pdns-recursor. I'm not sure implementing it only in dnsdist is enough.

includes individuals and 'other'

Public Hosted Service



May 25th GDPR enforcement

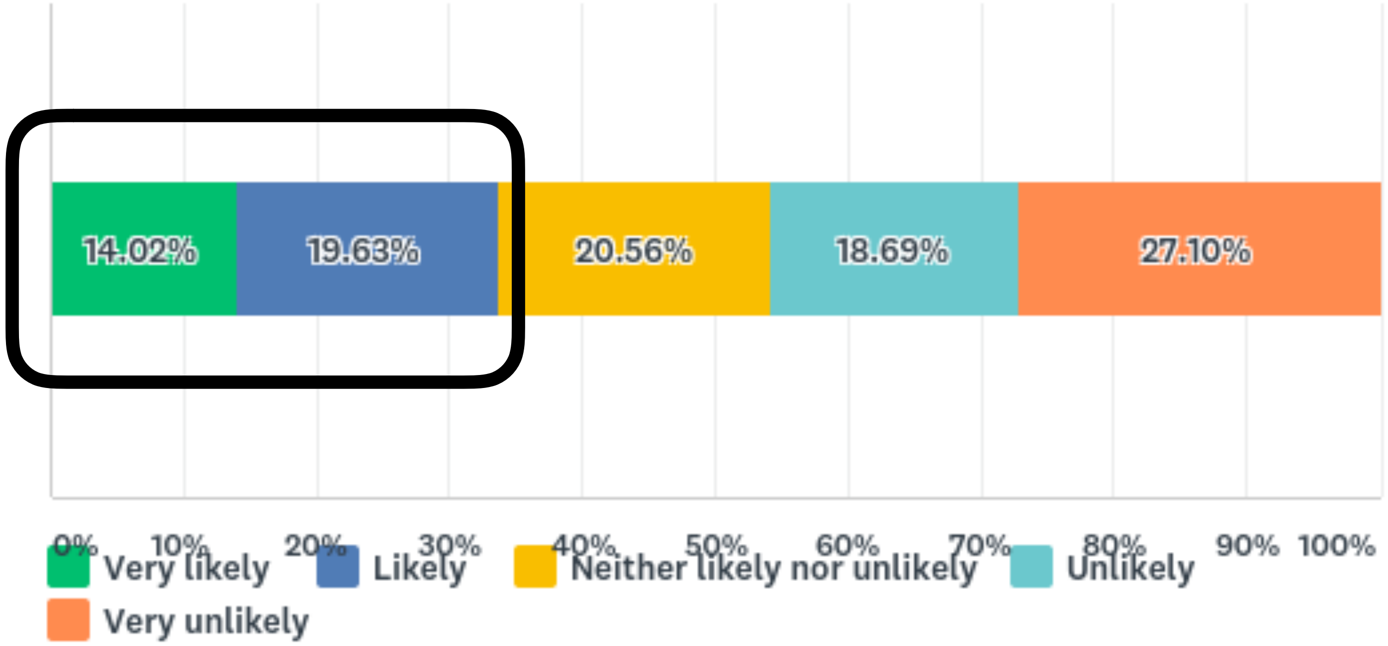
GDPR impact summary

- 35% think GDPR will impact DNS data processing
- 29% agree that QNAME minimization is required for GDPR - the exact same number disagree
- Website operators *loathe* the EU cookie law, think the notices are pointless and don't want to see a similar rule for DNS
- Many operators already have consent agreements, and several already minimize personal data storage and processing for privacy reasons.
- >20% of respondents think they can identify children's data (or block their use of their services)

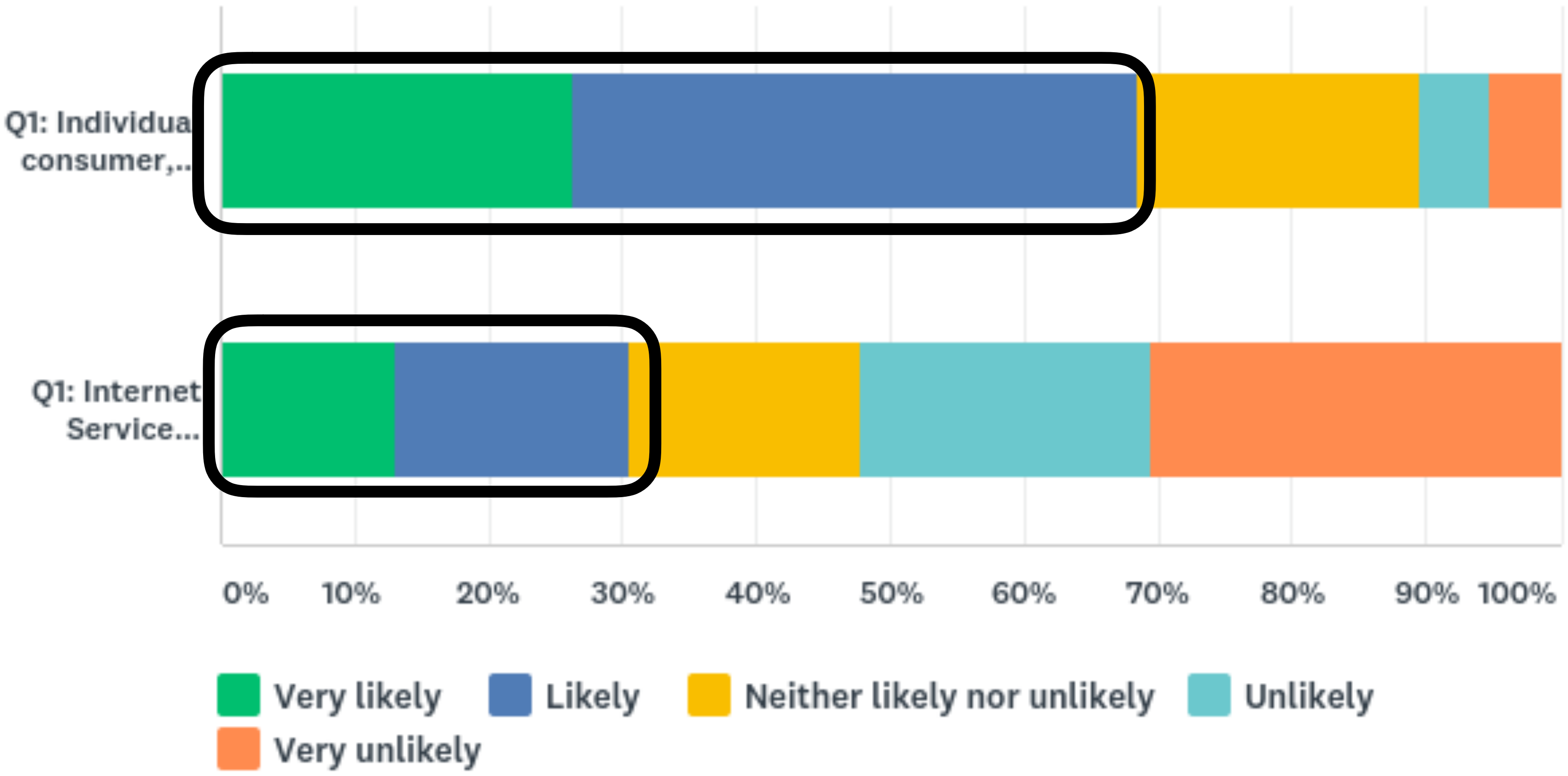
GDPR & DNS Data

Q11 GDPR Article 21 "Right to Object", states that an individual has the Right to Object to the processing of their data for direct marketing purposes. Do you expect that this provision will change how you store or process DNS data?

35% Likely



Individuals expect GDPR to have more impact on DNS

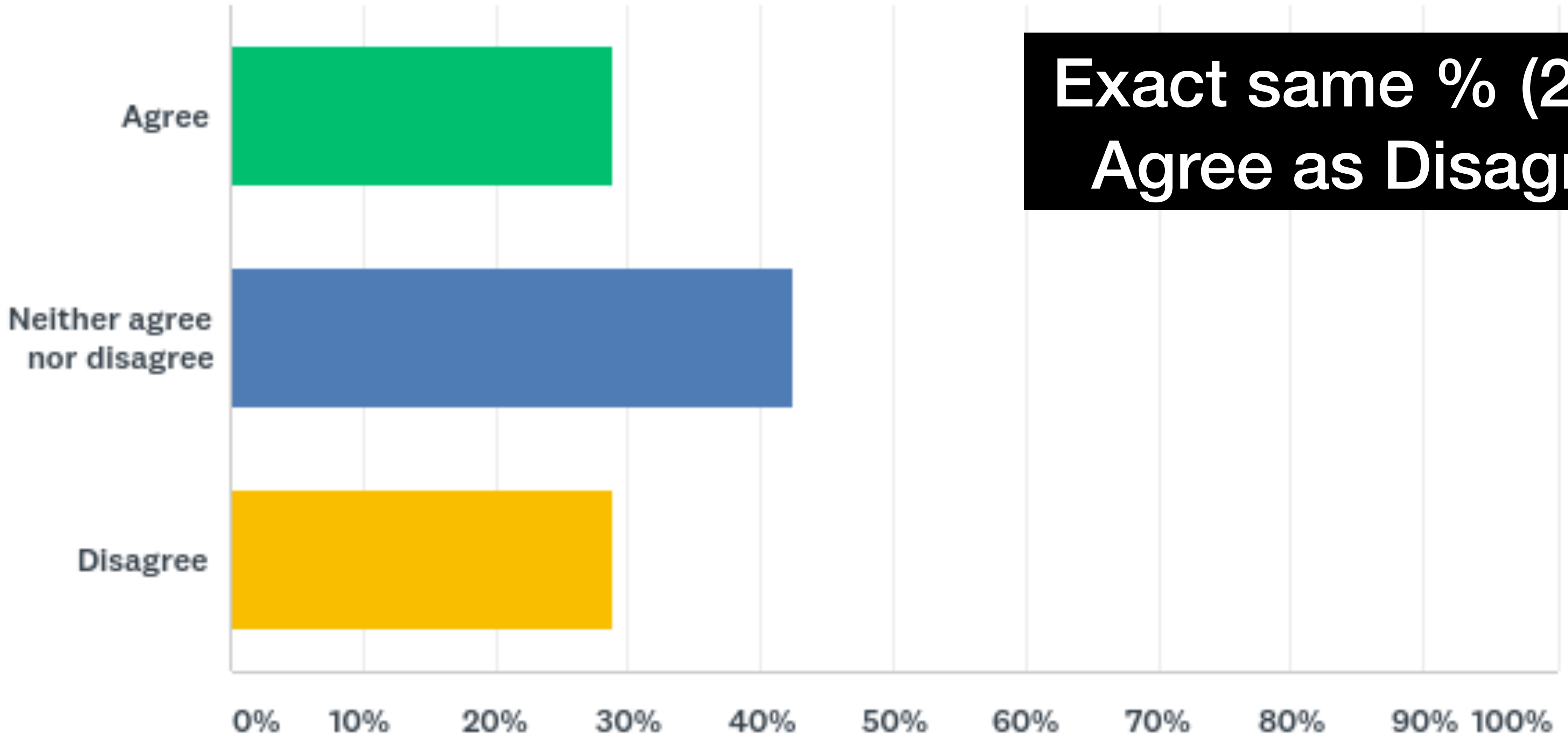


comparing Individuals with Internet Service Providers

Do you believe that QNAME minimization is required in order to comply with GDPR Article 25?

GDPR Article 25 (2):
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

Is QNAME Minimization required for GDPR?



Exact same % (29%) Agree as Disagree

excludes individuals and ‘other’

DNS Privacy Consent ala Cookies

This is an excellent example of policy developers being completely out of touch with the necessary intricacies of how the DNS actually works.

The EU Cookie Law was a terrible idea, needs to be revoked. Users don't care about notifications.

Fuck the EU Cookie Law. All websites are awful with the cookie notice. EU is legal nightmare. We should all use uBlock Origin, and go to a whisky party instead of losing time with this. Let's encrypt the DNS over TLS. We'll see what's left after.

That would be crazy. The EU Cookie Law is already terrible because it's the wrong solution to a perceived-yet-overstated problem that is specific to HTTP/HTTPS. Adding more warnings for users concerning DNS is only going to add confusion and drive them crazy in every application that they use -- the "free convenience" that the internet provides today will become a thing of the past and people will find it to be more of a nuisance if this were to happen (this would be a very terrible thing for the internet).

There are too many actors in the resolution chain to both get and signal user consent. Few end users know the DNS exists. Proposed regulation like this would be unworkable. Legislators need to be told that.