Recipient-Accountable Private Personal Data (RAPPD)

Yuan Kang, Allan Schiffman, Jeff Shrager

Columbia, CommerceNet, Stanford

May 17, 2014

1. Challenges for the user
2. What RAPPD does
3. How RAPPD works

Unclear Privacy Assumptions

Ask and you shall receive.

Unclear Privacy Assumptions

~~Ask and you shall receive.~~
Ask and you might receive.

Unclear Privacy Assumptions

~~Ask and you shall receive.~~
~~Ask and you might receive.~~
Don't ask, and you won't receive.

Unclear Privacy Assumptions

~~Ask and you shall receive.~~
~~Ask and you might receive.~~
Don't ask, and you won't receive.

1. Implicit

Unclear Privacy Assumptions

~~Ask and you shall receive.~~
~~Ask and you might receive.~~
Don't ask, and you won't receive.

1. Implicit
2. One-size fits all

Unclear Privacy Assumptions

~~Ask and you shall receive.~~
~~Ask and you might receive.~~
Don't ask, and you won't receive.

1. Implicit
2. One-size fits all
3. Context-dependent

Unclear Privacy Assumptions

~~Ask and you shall receive.~~

~~Ask and you might receive.~~

Don't ask, and you won't receive.

1. Implicit
2. One-size fits all
3. Context-dependent

Unclear Privacy Assumptions

~~Ask and you shall receive.~~

~~Ask and you might receive.~~

Don't ask, and you won't receive.

1. Implicit
2. One-size fits all
3. Context-dependent

Trust but verify.

Why Johnny (Inc.) Won't Encrypt

Recipient can refuse to setup system.

Why Johnny (Inc.) Won't Encrypt

Recipient can refuse to setup system.

1. Service sign-up

Why Johnny (Inc.) Won't Encrypt

Recipient can refuse to setup system.

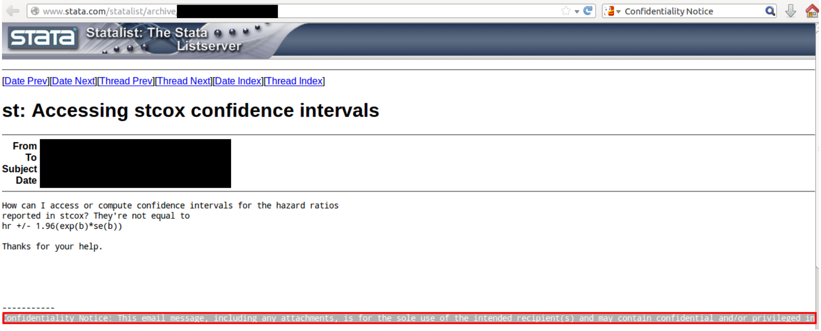
1. Service sign-up
2. Software Installation

Why Johnny (Inc.) Won't Encrypt

Recipient can refuse to setup system.

1. Service sign-up
2. Software Installation
3. Large, inflexible organizations

No Reading Allowed



www.stata.com/statalist/archive/[redacted]
Confidentiality Notice
STATA
Statalist: The Stata Listserver

[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

st: Accessing stcox confidence intervals

From
To
Subject
Date

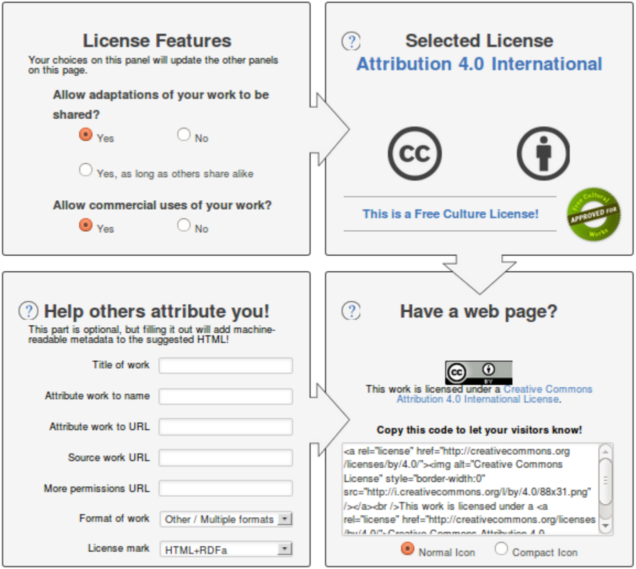
[redacted]

```
How can I access or compute confidence intervals for the hazard ratios
reported in stcox? They're not equal to
hr +/- 1.96(exp(b)*se(b))

Thanks for your help.



-----------
Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and/or privileged in
```

No Reading Allowed

Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. If you are not the intended recipient(s), you are hereby notified that any dissemination, unauthorized review, use, disclosure or distribution of this email and any materials contained in any attachments is prohibited. If you receive this message in error, or are not the intended recipient(s), please immediately notify the sender by email and destroy all copies of the original message, including attachments.

The CC Connection



License Features

Your choices on this panel will update the other panels on this page.

Allow adaptations of your work to be shared?

● Yes ○ No

○ Yes, as long as others share alike

Allow commercial uses of your work?

● Yes ○ No

Selected License

Attribution 4.0 International

This is a Free Culture License!

Help others attribute you!

This part is optional, but filling it out will add machine-readable metadata to the suggested HTML!

Title of work	
Attribute work to name	
Attribute work to URL	
Source work URL	
More permissions URL	
Format of work	Other / Multiple formats
License mark	HTML+RDFa

Have a web page?

This work is licensed under a Creative Commons Attribution 4.0 International License.

Copy this code to let your visitors know!

```
<a rel="license" href="http://creativecommons.org
/licenses/by/4.0/"><img alt="Creative Commons
License" style="border-width:0"
src="http://i.creativecommons.org/l/by/4.0/88x31.png"
/></a><br />This work is licensed under a <a
rel="license" href="http://creativecommons.org/licenses
/by/4.0/">Creative Commons Attribution 4.0
```

● Normal Icon ○ Compact Icon

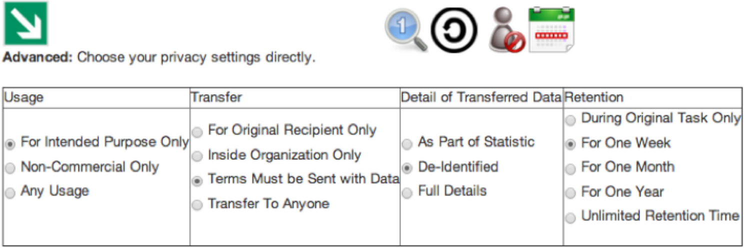
RAPPD Features

RAPPD Features

1. Clear privacy expectations: Expressed digitally and graphically

RAPPD Features

1. Clear privacy expectations: Expressed digitally and graphically

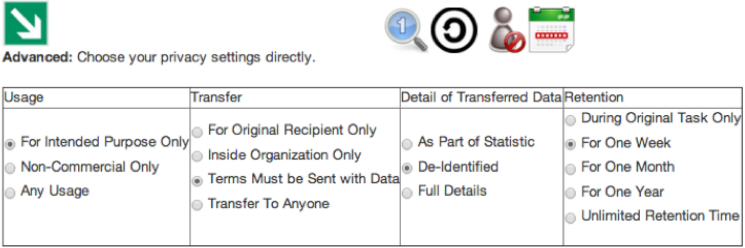


Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only	○ For Original Recipient Only	○ As Part of Statistic	○ During Original Task Only
○ Non-Commercial Only	○ Inside Organization Only	● De-Identified	● For One Week
○ Any Usage	● Terms Must be Sent with Data	○ Full Details	○ For One Month
	○ Transfer To Anyone		○ For One Year
			○ Unlimited Retention Time

RAPPD Features

1. Clear privacy expectations: Expressed digitally and graphically
2. Usage accounting:

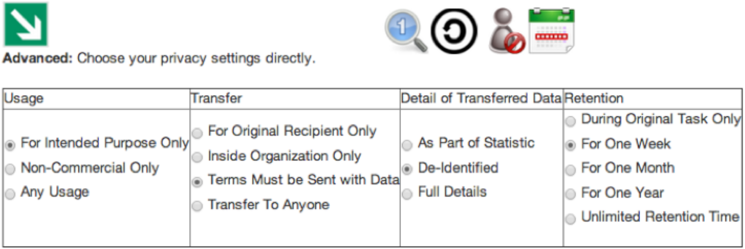


Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only ○ Non-Commercial Only ○ Any Usage	○ For Original Recipient Only ○ Inside Organization Only ● Terms Must be Sent with Data ○ Transfer To Anyone	○ As Part of Statistic ● De-Identified ○ Full Details	○ During Original Task Only ● For One Week ○ For One Month ○ For One Year ○ Unlimited Retention Time

RAPPD Features

1. Clear privacy expectations: Expressed digitally and graphically
2. Usage accounting:
    1. First recipient always tracked

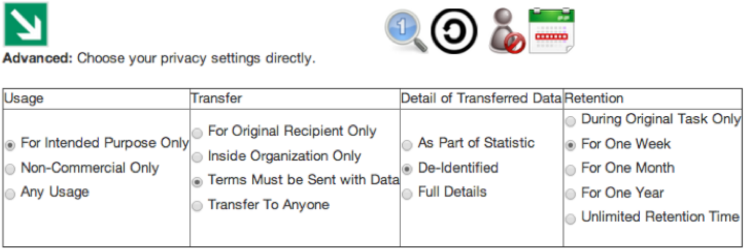


Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only ○ Non-Commercial Only ○ Any Usage	○ For Original Recipient Only ○ Inside Organization Only ● Terms Must be Sent with Data ○ Transfer To Anyone	○ As Part of Statistic ● De-Identified ○ Full Details	○ During Original Task Only ● For One Week ○ For One Month ○ For One Year ○ Unlimited Retention Time

RAPPD Features

1. Clear privacy expectations: Expressed digitally and graphically
2. Usage accounting:
   1. First recipient always tracked
   2. Support tracking of secondary recipients

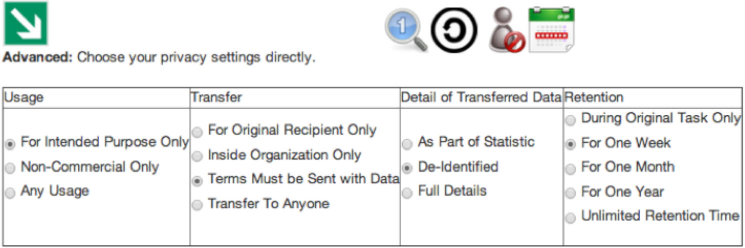


Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only ○ Non-Commercial Only ○ Any Usage	○ For Original Recipient Only ○ Inside Organization Only ● Terms Must be Sent with Data ○ Transfer To Anyone	○ As Part of Statistic ● De-Identified ○ Full Details	○ During Original Task Only ● For One Week ○ For One Month ○ For One Year ○ Unlimited Retention Time

RAPPD Features

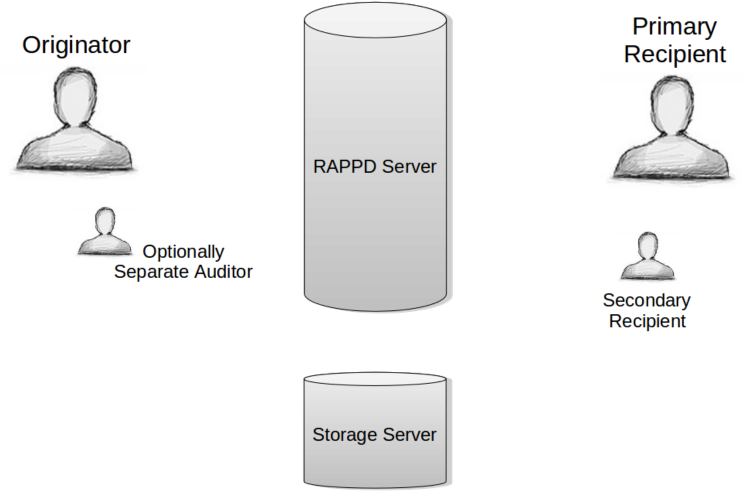
1. Clear privacy expectations: Expressed digitally and graphically
2. Usage accounting:
   1. First recipient always tracked
   2. Support tracking of secondary recipients
3. No extra setup: Uses existing web technologies



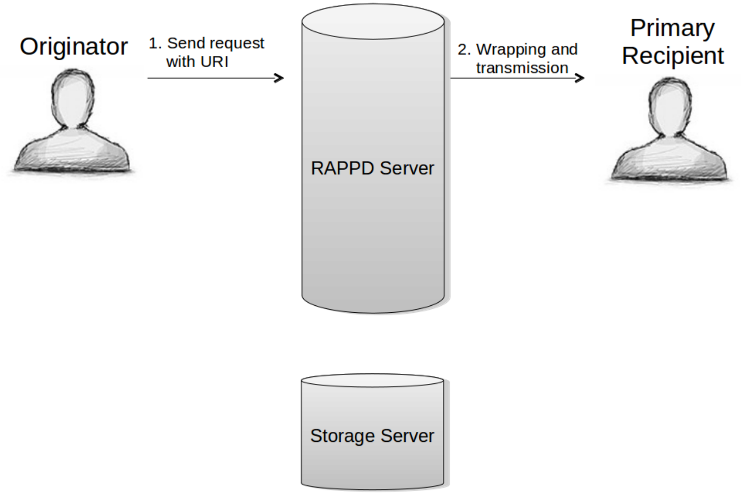
Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only ○ Non-Commercial Only ○ Any Usage	○ For Original Recipient Only ○ Inside Organization Only ● Terms Must be Sent with Data ○ Transfer To Anyone	○ As Part of Statistic ● De-Identified ○ Full Details	○ During Original Task Only ● For One Week ○ For One Month ○ For One Year ○ Unlimited Retention Time

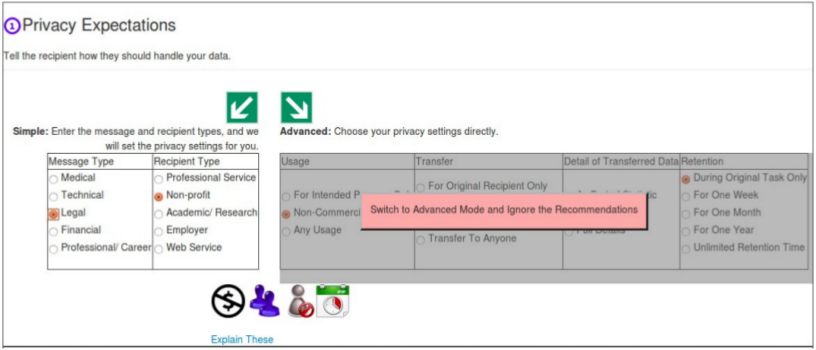
RAPPD Architecture



Sending


Originator
1. Send request with URI
RAPPD Server
2. Wrapping and transmission
Primary Recipient
Storage Server

Sending



Privacy Expectations

Tell the recipient how they should handle your data.

Simple: Enter the message and recipient types, and we will set the privacy settings for you.

Message Type	Recipient Type
○ Medical	○ Professional Service
○ Technical	● Non-profit
● Legal	○ Academic/ Research
○ Financial	○ Employer
○ Professional/ Career	○ Web Service

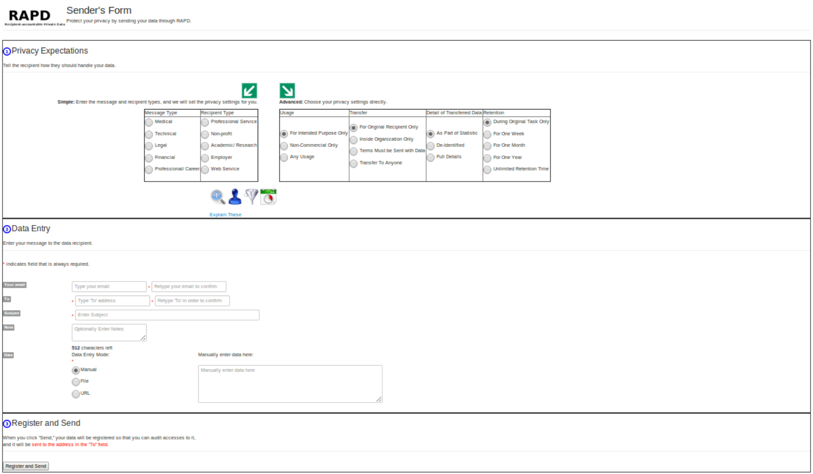
Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
○ For Intended P ● Non-Commerci ○ Any Usage	○ For Original Recipient Only ○ Transfer To Anyone		● During Original Task Only ○ For One Week ○ For One Month ○ For One Year ○ Unlimited Retention Time

Switch to Advanced Mode and Ignore the Recommendations

Explain These

Sending



RAPD
Recipient-accountable Private Data

Sender's Form

Protect your privacy by sending your data through RAPD.

①Privacy Expectations

Tell the recipient how they should handle your data.

Simple: Enter the message and recipient types, and we will set the privacy settings for you.

Message Type	Recipient Type
○ Medical	○ Professional Service
○ Technical	○ Non-profit
○ Legal	○ Academic/ Research
○ Financial	○ Employer
○ Professional/ Career	○ Web Service

Advanced: Choose your privacy settings directly.

Usage	Transfer	Detail of Transferred Data	Retention
● For Intended Purpose Only	● For Original Recipient Only	● As Part of Statistic	● During Original Task Only
○ Non-Commercial Only	○ Inside Organization Only	○ De-Identified	○ For One Week
○ Any Usage	○ Terms Must be Sent with Data	○ Full Details	○ For One Month
	○ Transfer To Anyone		○ For One Year
			○ Unlimited Retention Time

Explain These

②Data Entry

Enter your message to the data recipient.

* indicates field that is always required.

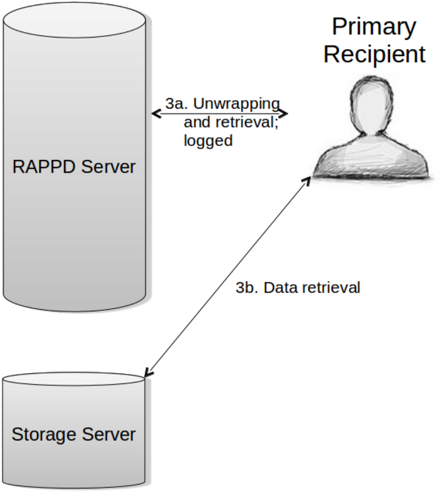
Your email	Type your email * Retype your email to confirm
To	* Type 'To' address * Retype 'To' in order to confirm
Subject	* Enter Subject
Note	Optionally Enter Notes 512 characters left
Data	Data Entry Mode: * ● Manual ○ File ○ URL Manually enter data here: Manually enter data here

③Register and Send

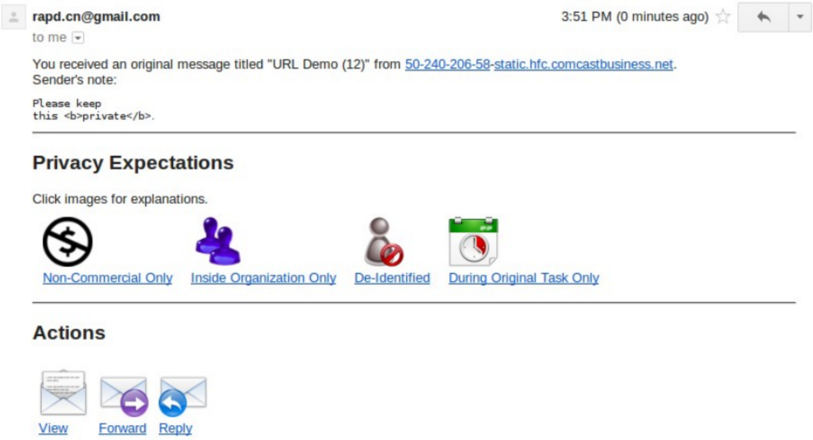
When you click "Send," your data will be registered so that you can audit accesses to it,
and it will be sent to the address in the "To" field.

Register and Send

Receiving


RAPPD Server
3a. Unwrapping and retrieval; logged
Primary Recipient
3b. Data retrieval
Storage Server

Receiving



rapd.cn@gmail.com
to me

3:51 PM (0 minutes ago)

You received an original message titled "URL Demo (12)" from 50-240-206-58-static.hfc.comcastbusiness.net.
Sender's note:

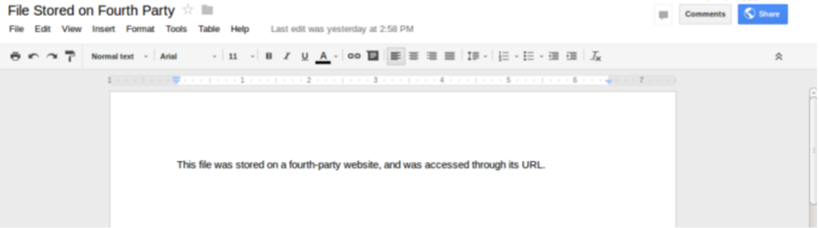
```
Please keep
this <b>private</b>.
```

Privacy Expectations

Click images for explanations.

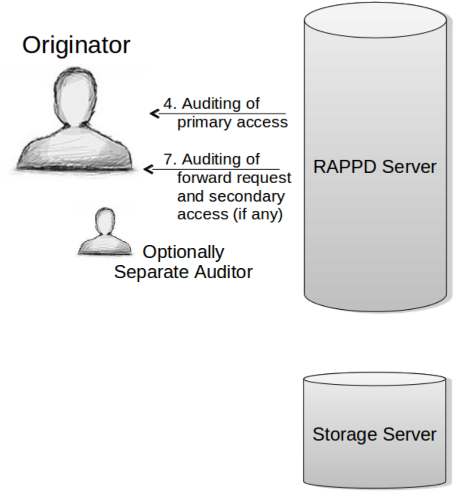
Actions

Receiving

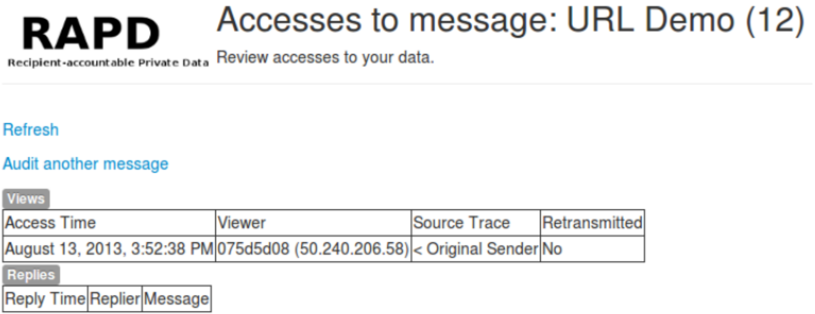


This file was stored on a fourth-party website, and was accessed through its URL.

Auditing


Originator
4. Auditing of primary access
7. Auditing of forward request and secondary access (if any)
Optionally Separate Auditor
RAPPD Server
Storage Server

Auditing



Accesses to message: URL Demo (12)

Review accesses to your data.

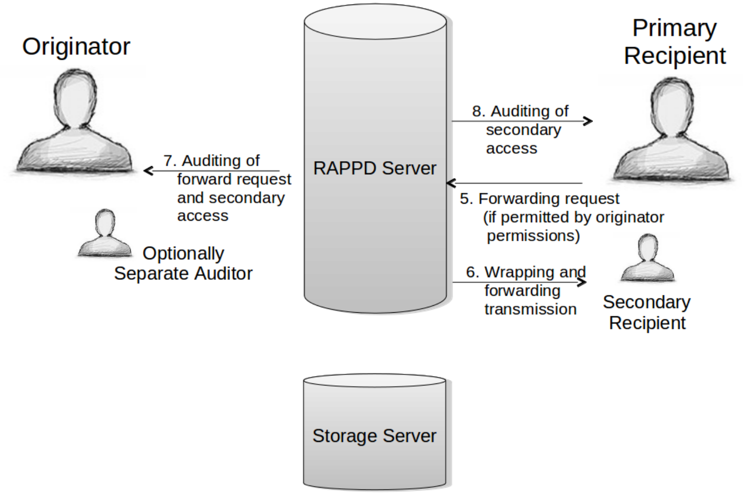
Views

Access Time	Viewer	Source Trace	Retransmitted
August 13, 2013, 3:52:38 PM	075d5d08 (50.240.206.58)	< Original Sender	No

Replies

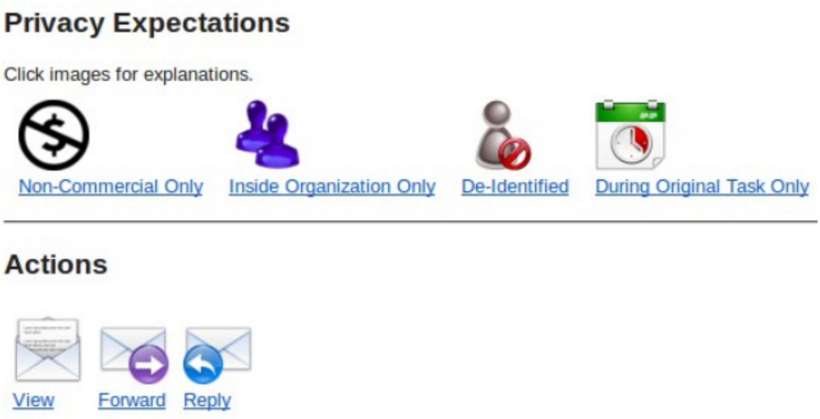
Reply Time	Replier	Message

Forwarding



Originator
Primary Recipient
RAPPD Server
8. Auditing of secondary access
7. Auditing of forward request and secondary access
5. Forwarding request (if permitted by originator permissions)
Optionally Separate Auditor
6. Wrapping and forwarding transmission
Secondary Recipient
Storage Server

Forwarding

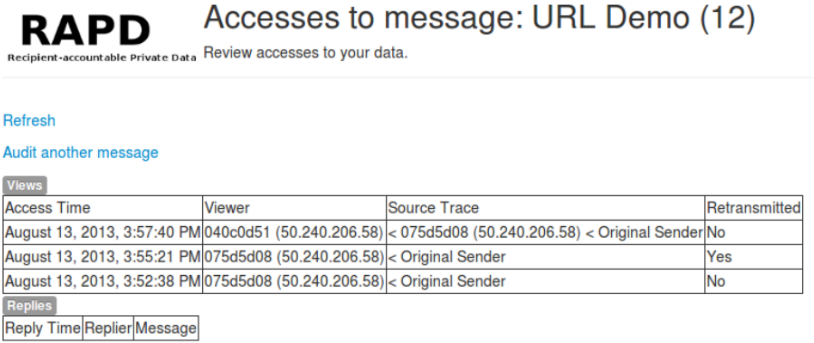


Privacy Expectations

Click images for explanations.

Actions

Forwarding



RAPD
Recipient-accountable Private Data

Accesses to message: URL Demo (12)

Review accesses to your data.

Refresh

Audit another message

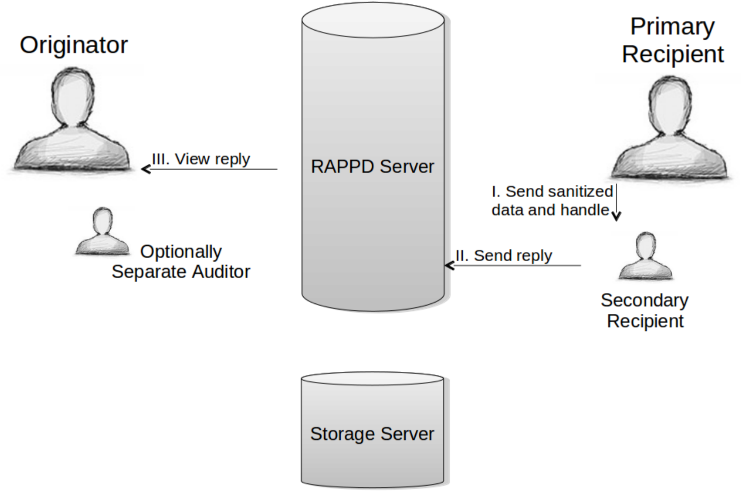
Views

Access Time	Viewer	Source Trace	Retransmitted
August 13, 2013, 3:57:40 PM	040c0d51 (50.240.206.58)	< 075d5d08 (50.240.206.58) < Original Sender	No
August 13, 2013, 3:55:21 PM	075d5d08 (50.240.206.58)	< Original Sender	Yes
August 13, 2013, 3:52:38 PM	075d5d08 (50.240.206.58)	< Original Sender	No

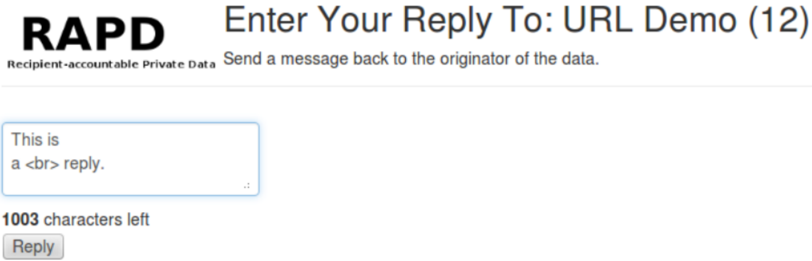
Replies

Reply Time	Replier	Message

Proxied Reply



Proxied Reply



RAPD

Recipient-accountable Private Data

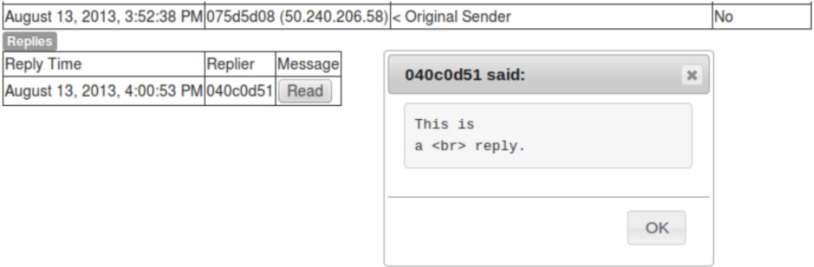
Enter Your Reply To: URL Demo (12)

Send a message back to the originator of the data.

This is
a <br> reply.

1003 characters left

Proxied Reply



August 13, 2013, 3:52:38 PM	075d5d08 (50.240.206.58)	< Original Sender	No

Replies

Reply Time	Replier	Message
August 13, 2013, 4:00:53 PM	040c0d51	Read

040c0d51 said:

```
This is
a <br> reply.
```

Recipient-Accountable Private Personal Data (RAPPD)

Recipient-Accountable Private Personal Data (RAPPD)

Don't ask, and you won't receive.

Recipient-Accountable Private Personal Data (RAPPD)

~~Don't ask, and you won't receive.~~
Ask, and you might receive.

Recipient-Accountable Private Personal Data (RAPPD)

~~Don't ask, and you won't receive.~~
Ask, and you might receive.

Trust but verify.

Recipient-Accountable Private Personal Data (RAPPD)

~~Don't ask, and you won't receive.~~
Ask, and you might receive.

Trust but verify.
Record and audit.