DATA PRIVACY DAY

Reporting on our first Privacy Research Experiment #1:

"Submitting Privacy Requests"

Introductions

Your Host: Craig Erickson, CISSP CISA
Data Protection Officer at PrivacyPortfolio

Craig Erickson has worked in cybersecurity for multiple firms as an Analyst, Engineer and IT Auditor for 8 years in Puget Sound and the San Francisco Bay Area.

Craig specializes in Data Governance, leveraging over 20 years of experience as a business process and systems integration expert.
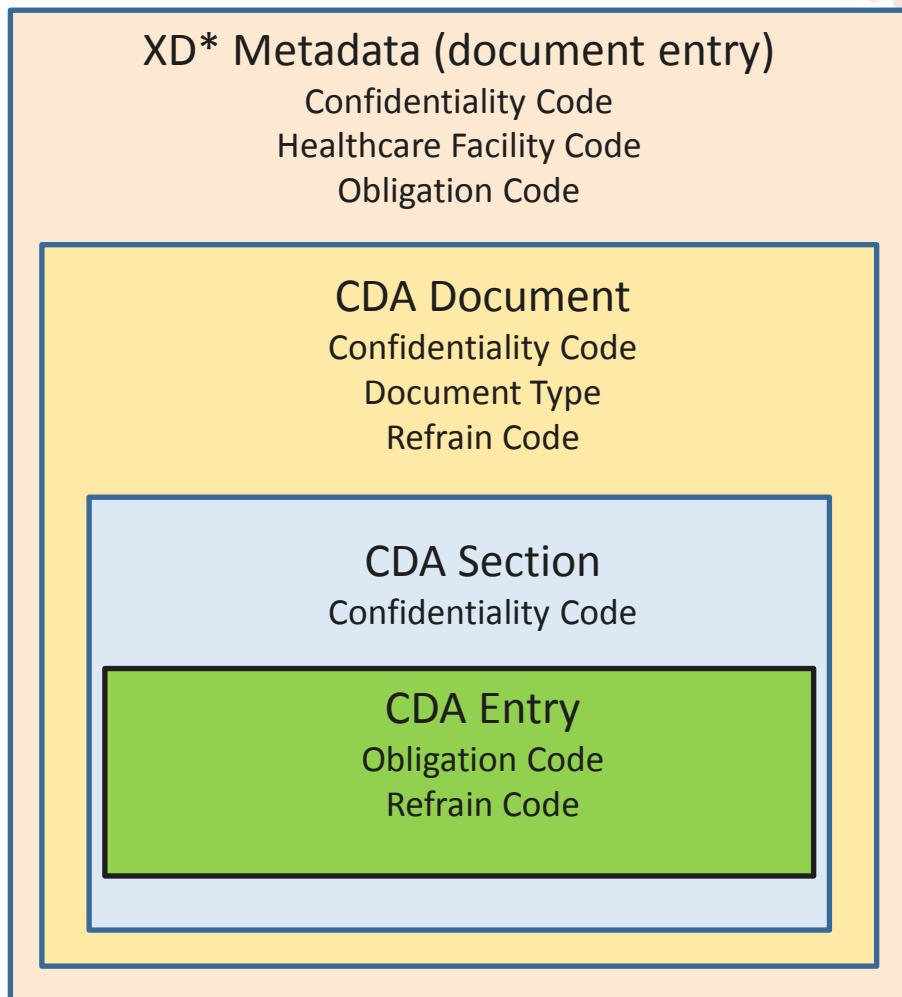
#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Introducing PrivacyPortfolio

XD* Metadata (document entry)
Confidentiality Code
Healthcare Facility Code
Obligation Code

CDA Document
Confidentiality Code
Document Type
Refrain Code

CDA Section
Confidentiality Code

CDA Entry
Obligation Code
Refrain Code

The proposed model relies on personal data stored in a secure repository, under the control of individual data subject who has an undisputed claim of ownership over their data assets.

An API is needed to provide a common interface to these repositories.

The goal is to automate services that supports privacy transactions between entities and individuals.

 # PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Agenda

10:00		Introductions
10:05		The Problem and Why We Should Care
10:10		Experiment #1 Methodology
10:15		Experiment #1 Results
10:25		Key Challenges, Issues & Concerns
10:35		Improvements
10:40		Q&A - Discussion

PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

iapp

News   Connect   Train   Certify   Resources   Conferences   Join   **STORE**

Data subject rights

Security of your information

Data storage and retention

Changes and updates to the Privacy Notice

Questions, concerns or complaints

Data Protection Officer

The IAPP is headquartered in New Hampshire, in the United States. The IAPP has appointed an internal data protection officer for you to contact if you have any questions or concerns about the IAPP's personal data policies or practices. The IAPP's data protection officer's name and contact information are as follows:

Rita Heimes
IAPP
75 Rochester Avenue
Portsmouth, New Hampshire, USA
dpo@iapp.org
+1 603-427-9200

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

What happens when we ask a question, express a concern, or lodge a complaint?

Who has the right to do so?

Why should we care about submitting privacy requests?

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

DATA PRIVACY DAY

iapp

News   Connect   Train   Certify   Resources   Conferences   Join   **STORE**

Data subject rights

Security of your information

Data storage and retention

Changes and updates to the Privacy Notice

Questions, concerns or complaints

Data Protection Officer

The IAPP is headquartered in New Hampshire, in the United States. The IAPP has appointed an internal data protection officer for you to contact if you have any questions or concerns about the IAPP's personal data policies or practices. The IAPP's data protection officer's name and contact information are as follows:

Rita Heimes
IAPP
75 Rochester Avenue
Portsmouth, New Hampshire, USA
dpo@iapp.org
+1 603-427-9200

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Notice. Consumers should be given notice of an entity's information practices before personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.

Choice. …means giving consumers options…

Access. …an individual's ability both to access personal data an entity possesses AND to contest the accuracy and completeness of personal data…

Security. …safeguards against unauthorized access, destruction, use or disclosure…

Enforcement. …core principles of privacy protection can only be effective if there is a mechanism in place to enforce them…

 # PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Let's try to make an informed decision as to whether and to what extent we choose to disclose personal information.

Can we access our data?

Are we able to enforce the security safeguards that protect our privacy?

What are our options...

LET'S GO MYSTERY SHOPPING!

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Privacy Portfolio

Data Privacy Day 2019 Champion Registration is now OPEN ‼ Click here to sign yourself or your business/organization up and receive a #PrivacyAware toolkit.

StaySafeOnline
Powered by: National Cyber Security Alliance

About   Blog   Events   News   Media Room   Contact   STOP. THINK. CONNECT.™

DATA PRIVACY DAY   STAY SAFE ONLINE   KEEP MY BUSINESS SECURE   GET INVOLVED   RESOURCES LIBRARY

Data Privacy Day 2019 Social Media Graphics

Shareable, non-proprietary images that help to promote Data Privacy Day and Privacy Awareness

Data Privacy Day

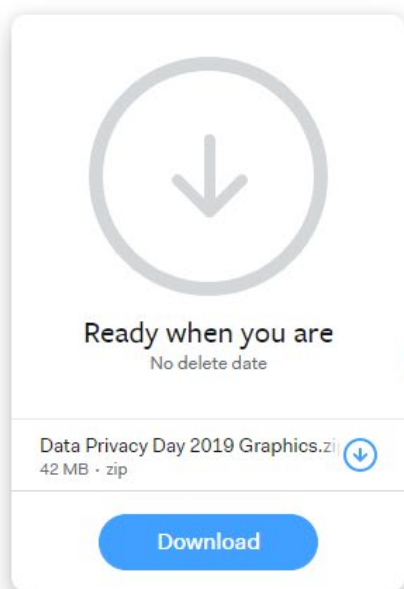WETRANSFER DOWNLOAD (.ZIP)   DOWNLOAD (.XLSX) THE SAMPLE POSTS

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

10

DATA PRIVACY DAY

Help   About us   Got Plus?

we

Ready when you are
No delete date

Data Privacy Day 2019 Graphics.zip
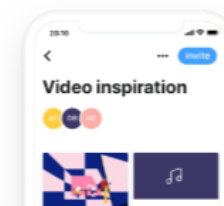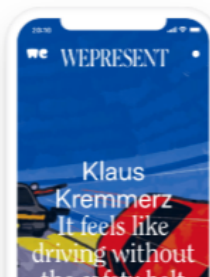42 MB · zip

Download

NATIONAL
CYBER**SECURITY**
ALLIANCE

https://ncsa.wetransfer.com/about

https://ncsa.wetransfer.com/downloads/

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

DATA PRIVACY DAY

Help | About us | WeTransfer | Products | Plus | Advertise | Got Plus?

Welcome to WeTransfer

WeTransfer was founded in 2009 as the simplest way to send big files around the world. Today we're a set of beautifully obvious tools that bring your ideas to life.

WEPRESENT

Klaus Kremmerz
It feels like driving without the safety belt

Art Island Project

Concept 1

Video inspiration

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Organizations spend a lot of resources on privacy practices

Many privacy practices add a lot of undesirable burdens

Some privacy practices offer very little value to all stakeholders

When any security or compliance requirement has little or no value, other requirements also tend to suffer under the same perception whether that is applicable or not

PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Experiment #1:   Methodology

Goals

Discover how effective organizations are in responding to Privacy Requests and Concerns from Data Subjects, and explore how can this information be used to improve privacy practices.

Questions

How much effort(cost) is involved in resolving privacy requests?
How useful are the responses for data subjects?
What issues and concerns arise in responding to requests?

Metrics

- % of organizations responding to Privacy Requests and Concerns
- Time elapsed from start-to-finish
- Relevancy scores of responses provided

#️⃣ **PrivacyAware**

STAYSAFEONLINE.ORG/DPD19-LIVE

Experiment #1:   Methodology

Sample 100 organizations with published privacy policies

Skew sample with SMEs in privacy, security, and compliance (47)

Exclude organizations without email contact info – no web forms

Half receive this Privacy Question (email subject line):

"How and when will I be notified if there is a data breach?"

Half receive this Privacy Concern (email subject line):

"I'm concerned about how and when I'll be notified of a data breach"

* Designed to test if concerns are handled differently than questions

#PrivacyAware

Experiment #1:   Results

10%	Undeliverable
16%	No response after 2 attempts within 17 days
13%	Acknowledged but not answered within 15 days

39%	of all requests are not answered
40%	Answers
01%	Error
02%	Disqualified
07%	Boilerplate FAQs
13%	Additional Questions

102%	Total Sample

Experiment #1:   Results

Relevance Scores – Highly relevant

Usefulness Scores – Fairly useful

Effort Scores – Mostly low

Who responds?

8	unknown
19	privacy
1	contracts
10	support
2	exec
40	

Who responds better?

Team	Relevance	Usefulness	Effort
support	3	3	1
privacy	2	1	1

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Experiment #1:   Results

Most Frequent Responses:

22	general when and how
5	general when, specific how
6	specific when and how
0	specific when, general how

https://github.com/PrivacyPortfolio/Experiments/

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Key Challenges

Who are you? What is your relationship with us?

What is your question or concern?

Requirements to use web forms and account portals

Translating legal and policy language for end-users (lay people)

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Issues & Concerns

Role Context Issues

Security Concerns

Unqualified Respondents

Ethical Concerns

Notification Protocols

#PrivacyAware

STAYSAFEONLINE.ORG/DPD19-LIVE

Improving Privacy Practices

1. Revise our Policy to avoid specifying rights and contacts specific to role contexts of data subjects.

2. Modify our Privacy Request Templates to clearly state the role, relationship, and right to submit a request by or on behalf of the data subject.

3. Adopt a new policy rule that communication exchanges must not rely on data entry in online web forms or notices posted on websites.

4. The only valid responses are documented in writing and signed by a real person with title or appropriate group alias such as privacy, security, compliance.

Q&A / Open Discussion

PRIVACY IS GOOD FOR BUSINESS

UPDATE YOUR PRIVACY SETTINGS THIS DATA PRIVACY DAY (JANUARY 28)

DATA PRIVACY DAY

LEARN MORE
staysafeonline.org/data-privacy-day

JANUARY 28

ARE YOU AIRING DIRTY LAUNDRY?

UPDATE YOUR PRIVACY SETTINGS THIS DATA PRIVACY DAY (JANUARY 28)

DATA PRIVACY DAY

LEARN MORE
staysafeonline.org/data-privacy-day

JANUARY 28