Security and Privacy Considerations in Digital Death

Locasto, Massimi, DePasquale

NSPW 2011

Security and privacy considerations in digital death

Locasto, Massimi, DePasquale

QUIZ

No IRB

Refuse if you want

Results @ end

Preamble

Let's refrain from swimming in legal waters unless we know what specific sharks we're dealing with

International perspectives / anecdotes / insights welcome

Main Point

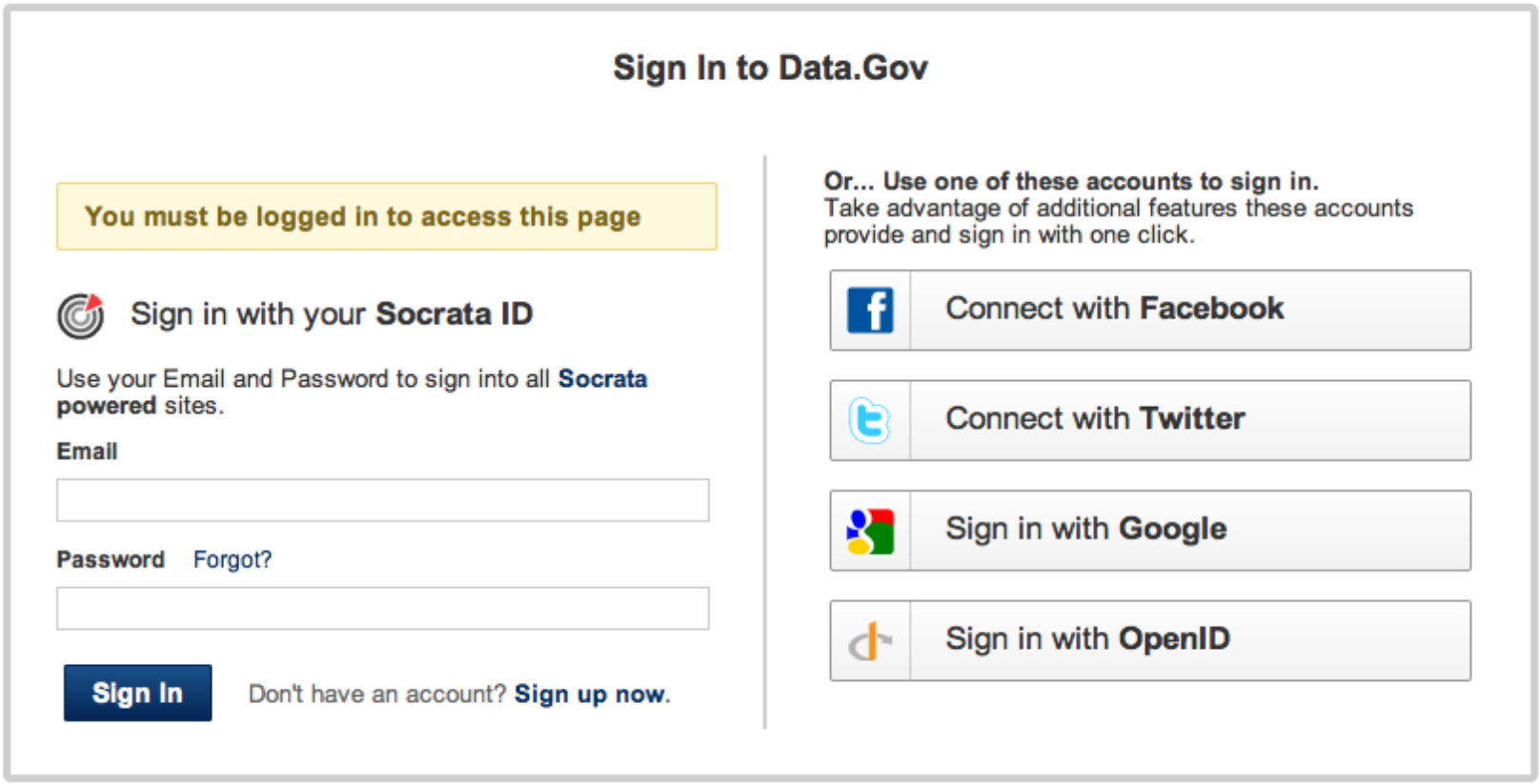
The accrual of a heterogeneous, distributed digital identity footprint presents unique and interesting authentication, authorization, and privacy issues — particularly related to how such an identity collection should be retired after a person dies.

We have a lot of authentication trash – and we don't know what to do with it

Boss: we need security

Underling: /googles for "HTML password form"

WTF?


METRICS
OPEN DATA SITES
GALLERY
WHAT'S NEW
Sign In to Data.Gov
You must be logged in to access this page
Sign in with your Socrata ID
Use your Email and Password to sign into all Socrata powered sites.
Email
Password
Forgot?
Sign In
Don't have an account? Sign up now.
Or... Use one of these accounts to sign in.
Take advantage of additional features these accounts provide and sign in with one click.
Connect with Facebook
Connect with Twitter
Sign in with Google
Sign in with OpenID

Authentication now pollutes our online experience.

Epsilon E-Mail Hack: How You Can Protect Yourself

By Bill Snyder, CIO
April 11, 2011 10:48 AM ET

Add a comment Print Like +1 0

Most of the time I only hear from my credit card companies when I owe them money or when they want to sell me a new service. That's changed; now I'm being bombarded with notes telling me that a company I never heard of has been successfully hacked and these still unknown bad guys now have my name and e-mail address -- and maybe more

Epsilon E-Mail Hack: How You Can Protect Yourself

By Bill Snyder, CIO
April 11, 2011 10:48 AM ET

Add a comment Print Like +1 0

Most of the time I only hear from my credit card companies when I owe them money or when they want to sell me a new service. That's changed; now I'm being bombarded with notes telling me that a company I never heard of has been successfully hacked and these still unknown bad guys now have my name and e-mail address -- and maybe more

Air Miles among firms hit by huge data breach

CBC News Posted: Apr 5, 2011 11:16 AM ET | Last Updated: Apr 6, 2011 8:01 AM ET 112

A growing list of companies including giant rewards firm Air Miles and hotelier Marriott are

Stay Connec

Epsilon E-Mail Hack: How You Can Protect Yourself

By Bill Snyder, CIO
April 11, 2011 10:48 AM ET

April 5, 2011

TIAA-CREF has been informed by Epsilon, a vendor we use to send emails, that files containing the first names, last names and email addresses of some TIAA-CREF participants were accessed without authorization.

We have not shared any participant account or financial information with Epsilon. So, this incident has not compromised your TIAA-CREF accounts and they remain secure. For your security, however, we wanted to call this matter to your attention.

As always, do not reply to emails asking for your personal information, account numbers or any other type of confidential information. TIAA-CREF will never ask for your personal information or login credentials in an email.

Below are some additional precautions we recommend you follow:

- Do not give your TIAA-CREF user ID or password in email.
- Do not respond to emails that require you to enter personal or financial information directly into the email.
- Do not reply to emails asking you to send personal information.
- Do not use your email address as a login ID or password.
- Do not respond to emails threatening to close your account if you do not provide personal information

We regret any inconvenience this may have caused and will keep you informed of relevant updates. For more information on TIAA-CREF's commitment to keeping your personal information secure, please visit: http://www.tiaa-cref.org/public/about/inside/topics/index.html?tc_lnk=bottomutlity&tc_mcid=emepsilon0411.

A growing list of companies including giant rewards firm Air Miles and hotelier Marriott are

Stay Connec

Epsilon E-Mail Hack: How You Can Protect Yourself

By Bill Snyder, CIO
April 11, 2011 10:48 AM ET

April 5, 2011

TIAA-CREF has been inforr
email addresses of some Tl

We have not shared any pa
TIAA-CREF accounts and tl

As always, do not reply to e
information. TIAA-CREF wil

Below are some additional

- Do not give you
- Do not respond
- Do not reply to
- Do not use you
- Do not respond

We regret any inconvenien
TIAA-CREF's commitment t
public/about/inside/topics/ir

BEST BUY | rewardzone MYRZ.COM BESTBUY.COM

Dear Valued Best Buy Customer,

On March 31, we were informed by Epsilon, a company we use to send emails to our customers, that files containing the email addresses of some Best Buy customers were accessed without authorization.

We have been assured by Epsilon that the only information that may have been obtained was your email address and that the accessed files did not include any other information. A rigorous assessment by Epsilon determined that no other information is at risk. We are actively investigating to confirm this.

For your security, however, we wanted to call this matter to your attention. We ask that you remain alert to any unusual or suspicious emails. As our experts at Geek Squad would tell you, be very cautious when opening links or attachments from unknown senders.

In keeping with best industry security practices, Best Buy will never ask you to provide or confirm any information, including credit card numbers, unless you are on our secure e-commerce site, www.bestbuy.com. If you receive an email asking for personal information, delete it. It did not come from Best Buy.

Our service provider has reported this incident to the appropriate authorities.

We regret this has taken place and for any inconvenience this may have caused you. We take your privacy very seriously, and we will continue to work diligently to protect your personal information. For more information on keeping your data safe, please visit: http://www.geeksquad.com/do-it-yourself/tech-tip/six-steps-to-keeping-your-data-safe.aspx.

Sincerely,

A growing list of companies including giant rewards firm Air Miles and hotelier Marriott are

Stay Connec

Epsilon

By Bill Snyder, CI

April 11, 2011 10:

April 5, 2011

TIAA-CREF has b

email addresses

We have not shar

TIAA-CREF accou

As always, do not

information. TIAA-

Below are some a

- Do nc
- Do nc
- Do nc
- Do nc
- Do nc

We regret any inconvenience t

TIAA-CREF's commitment to ke

public/about/inside/topics/index.html?tc_link=bottomutility&tc_mcid=emepsilon0411.

Add to Address Boo

Marriott

find a hotel

EXPLORE &

April 4, 2011

Dear Marriott Customer,

We were recently notified by Epsilon, a marketing vendor used by Marriott International, Inc. to manage customer emails, that an unauthorized third p access to a number of Epsilon's accounts including Marriott's email list.

In all likelihood, this will not impact you. However, we recommend that you to be on the alert for spam emails requesting personal or sensitive informa Please understand and be assured that Marriott does not send emails requ customers to verify personal information.

We take your privacy very seriously. Marriott has a long-standing commitm protecting the privacy of the personal information that our guests entrust to regret this has taken place and apologize for any inconvenience.

Please visit our FAQ to learn more.

Sincerely,

Marriott International, Inc.

t Yourself

MYRZ.COM BESTBUY.COM

send emails to our customers, that files accessed without authorization.

ay have been obtained was your email mation. A rigorous assessment by vely investigating to confirm this.

ttention. We ask that you remain alert to would tell you, be very cautious when

r ask you to provide or confirm any secure e-commerce site, rmation, delete it. It did not come from

authorities.

have caused you. We take your otect your personal information. For

http://www.geeksquad.com/do-it-yourself/tech-tip/six-steps-to-keeping-your-data-safe.aspx.

Sincerely,

s and

our

on

E-MAIL BREACH

A growing list of companies including giant rewards firm Air Miles and hotelier Marriott are

Stay Connec

Home > News > Digital media

September 22, 2006 4:00 AM PDT

Taking passwords to the grave

By Elinor Mills

Staff Writer, CNET News

Related Stories

William Talcott, a prominent San Francisco poet with dual Irish citizenship, had fans all over the world. But when he died in June of bo

FAMILY VALUE | JULY 23, 2011

PINs That Needle Families

Article | Comments (10)

Email | Print | Save | Like 131 | +1 3 | A A

Taking 15 minutes now to jot down your online passwords could save your family hours of frustration after you are gone.

As we all know, large chunks of our lives, both financial and personal, are lived online—bank statements, stock trades and email archives are all available with a few keystrokes. But when people die, their passwords often go with them, along with access to their digital assets.

Leon LaBrecque, a certified financial planner in Troy, Mich., says he has encountered the problem with a number of clients, including one who also was a friend who died of cancer. Mr. LaBrecque's friend had told him that his financial records were on his computer, but when the planner asked the client's wife for his password, she didn't know it.

"I looked at the dog sitting in the chair next to the computer, and typed in his name, Pepper. It worked, but I've been in other situations where we've had to hire a computer programmer to get into a hard drive," Mr. LaBrecque says.

He is encouraging clients to fill out a free form that includes user names and passwords to

lifehacker

DEATHHACKER

What Should I Do About My Virtual Life After Death?

Dear Lifehacker,

What Sh
Death?

BY JASC

Share

Blogger announces own death after battle with cancer

By Katie Silver, CNN
May 9, 2011 12:44 p.m. EDT

STORY HIGHLIGHTS

- A man leaves a post-mortem message published after his battle with cancer
- "Here it is. I'm dead," read the last internet post of Derek Miller
- News of Miller's death and his final post online went viral

(CNN) -- A Canadian man who blogged about his battle with cancer has died, but not without leaving a post-mortem message.

"Here it is. I'm dead," read the last internet post of Derek K. Miller, who died last week after more than four years of blogging about his struggle with colorectal cancer.

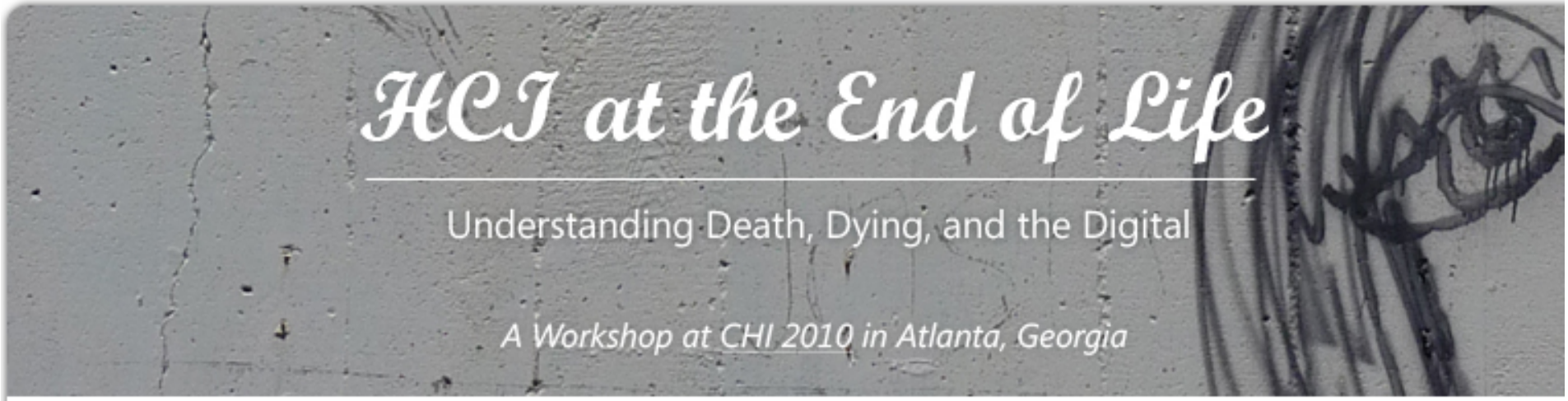
"In advance, I asked that once my body finally shut down from the punishments of my cancer, then my family and friends publish this prepared message I wrote -- the first part of the process of turning this from an active website to an archive," he wrote on his blog, penmachine.com.

A day after his death, a longtime friend, Alistair Calder, published the final message.

"I felt as though I was putting Derek's ... last moments on the web," Calder said. "It was really, really, really hard."

HOW DO WE MANAGE THIS IDENTITY FOOTPRINT?

Thanatosensitive Design



News

Description

Themes

- Mar 19, 2010: Schedule posted.
- Join our group on Facebook!
- Feb 12, 2010: Position papers posted.

Yahoo! Steps Up

"No Right of Survivorship and Non-Transferability. You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted."

Anyone Else?

Anyone Else?

How to Contact Twitter About a Deceased User

Tweet

In the event of the death of a Twitter user, we can close the account and help family members recover public Tweets from the account.

Please provide us the following:

1. Your first and last name, contact information (including email address), and your relationship to the deceased person.
2. The username of the Twitter account, or a link to the account's public profile page.
3. A link to a public obituary article.

You may contact us at privacy@twitter.com, by fax, or by mail at the following address :

Twitter Inc.,
c/o: Trust & Safety
795 Folsom Street, Suite 600
San Francisco, CA 94107
Fax : 415-222-9958

We will answer by email while specifying which information is needed.

We may not hand over access to the account, or share any non public information related to the account.

No Cohesion

Category	Service	Death/Transfer Clause
Email {US, UK, Canada}	Gmail, Hotmail, Yahoo	No, No, Yes
Social {US, UK, Canada}	Facebook, G+, LinkedIn	No, No, No
Ehealth {US}	MS Health Vault, Google Health	Yes, No
Banking {US, Canada}	USAA, BoA, Wells Fargo, Citibank, Scotia, BMO, RBC	No*, No, Yes*, Yes, No
Cloud Services {US}	Amazon, Google, MS	No, Yes, No

Discussion

Don’t store data in the first place.

Proactive deletion.

Unified ID management. <shudder>

Fine-grained delegation of DigitalID inheritance.

Sum Up

Death throws a curveball for security design, but we may have the technology to mostly handle this kind of event with proper planning and forethought.

Our Digital Footprints are way too large.

BACKUP

Definition of Digital Identity

We see identity as including (1) credentials (i.e., usernames, passwords, passphrases, email addresses, public keys, certificates, identifiers, roles, password "hint" questions and answers, SiteKey phrases and pictures) used to authenticate to the service and authorize different uses, (2) user preferences for interacting with that online identity, (3) personal information (i.e., names, account num- bers, address, contact information, date of birth, sex) stored by the service, and (4) content (e.g., account balances, comments, links, likes, posts, medical ailments) generated during the interaction of the user with the service.