September 14, 2017

Hacking Healthcare

TLP White
Policy Analysis – How a bill becomes a law

After years of debate (or at least threat of debate) on a Federal data breach notification law, Congress has approached the subject with a new sense of energy in the wake of the Equifax breach. The breach, which may have exposed PII of 143 million Americans, is most notable for how poorly the company handled the announcement and response. It announcing the breach nearly 2 months after discovery and providing unclear, unhelpful, and potentially deceptive notification it provided to those potentially involved. Otherwise, it was just another ho-hum theft of nearly half the country's PII that occurred as the result of unpatched, known vulnerabilities in poorly architected legacy systems.

So what is Congress going to do about it?

Well, they will hold a few hearings and demand answers with feigned outrage. We've seen this before, but it has not led to meaningful reform of breach notification or the legal and economic structure that facilitates the lax approach to security we saw at Equifax. There's not much reason to think this breach will elicit a different response from Washington. But it is worth noting that the White House has said they will look into new regulations to protect consumers from the impact of such breaches.

Federal Data Breach Notification – Back in 2011 and then again in 2015, the Obama Administration put forward legislative proposals to create a Federal data breach notification standard. These proposals were constructed so as not to "pre-empt" the 47 state laws (good comparison tool here) already in place, or specific industry regulations. As a result, the scope was pretty narrow, which was viewed as the only way to get a law passed. But even such a limited Federal approach didn't make any headway in Congress, despite a series of large scale breaches. Various bills from different Congressional committees have been introduced since, but none have made serious progress towards becoming law.

Of course, the healthcare industry already has federal laws around data breach notification in HIPAA and HITECH. There's not much momentum behind any talk of reforming HIPAA or HITECH.

Healthcare legislation – In healthcare legislation, the big push seems to be around increasing access and reducing costs to telemedicine for Medicare recipients – the house and senate both have packages moving through committee and bi-partisan support for getting something done. The Senate's CHRONIC bill has been hotlined and looks like it will move to the floor quickly. There's also an amendment in the package that will soften meaningful use requirements under HITECH. And broader health reform continues to percolate as an idea more than anything else – with Bernie Sanders introducing a Medicare-for-all bill.

September 14, 2017

Hot Links –

DHS issues a Binding Operational Directive (BOD) ordering all civilian agencies to cease use of Kaspersky products – acting Secretary Elaine Dukes issued this directive today, citing concerns over Kaspersky's relationship to the Russian government and Russian laws that might compel Kaspersky to provide sensitive accesses or information to the Russian government.
--[from July] Kaspersky Lab Has Been Working With Russian Intelligence (Bloomberg)
--Kaspersky software banned from US government agencies (Ars)
--Under scrutiny, Kaspersky Lab considers changes to U.S. subsidiary (Reuters)

NIST puts out a guide on "recovering from ransomware and other destructive events" – this is an interesting approach from NIST's National Cybersecurity Center of Excellence that takes a lot of the content and approach from the NIST Framework and applies it specifically to a certain challenger – in this case ransomware and other destructive malware. Comment period is open until November 6 – Let us know if you have thoughts!

The Energy Department funds cybersecurity grants – could a shift to "resilience" grants be the future for a program such as "Meaningful Use?" HHS has focused grant money on security in health care, but it has largely been at the sector level. DOE is showing that an incentive based approach can be directed at secure/resilient technology development and adoption.

Canada and Massachusetts are suing Equifax.

HHS CISO: 3 things hospitals should do right now to strengthen cybersecurity (healthcare IT news) – key quote: "If you have the ability, then jump into the NH-ISAC," Wlaschin said here at the Healthcare Security Forum on Tuesday. "They can help. It's not just compliance, it's also about preparedness and resilience."

How HIPAA Rules Apply with Law Enforcement Investigations (Health IT Security) – an interesting look at how health care companies should think about providing patient data when law enforcement requests it. A couple weeks ago we discussed how companies should think about HIPAA obligations when voluntarily providing cyber-threat indicators to the FBI. This is a nice complement.

The Week Ahead –

Conferences and Webinars –
--HIMSS Healthcare Security Forum (9/11-13)
--Billington CyberSecurity Summit (9/13)
--Basic Best Practices in Cybersecurity - Alabama (NH-ISAC) (9/15)
--Health IT Summit - St. Petersburg, FL (NH-ISAC) (9/20)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)

Reports –
--Cyber Threat Data Sharing Needs Refinement (Lexington Institute)

September 14, 2017

--Study: In 11-Hour Workday, Docs Spend 6 Hours on EHR Tasks (Annals of Family Medicine via healthcare informatics)

Sundries –

Policy:

--Protect, respond, collaborate, deter: a new opportunity for European cybersecurity (Microsoft)
--China beefs up cyber defenses with centralized threat database (Reuters)
--DHS S&T Awards $8.6 Million for Five Mobile Application Security R&D Projects (DHS)
--Remember the artist who had his iPhone searched at the border? He's now suing (Ars)
--'There Is Still Hope - Even for Me' – Snowden interview (Der Spiegel)
--Martin Shkreli is headed to jail (Ars)

Op-eds:

--How the U.S. can counter threats from DIY weapons and automation (Michael Dempsey - Wired)

Tech:

--Just the good stuff from Tuesday's iPhone event (Digg)
--I'm worried that FaceID is going to suck—and here's why (Ars)

Threats:

--New Kedi RAT Uses Gmail to Exfiltrate Data (Security Week)

Vulnerabilities:

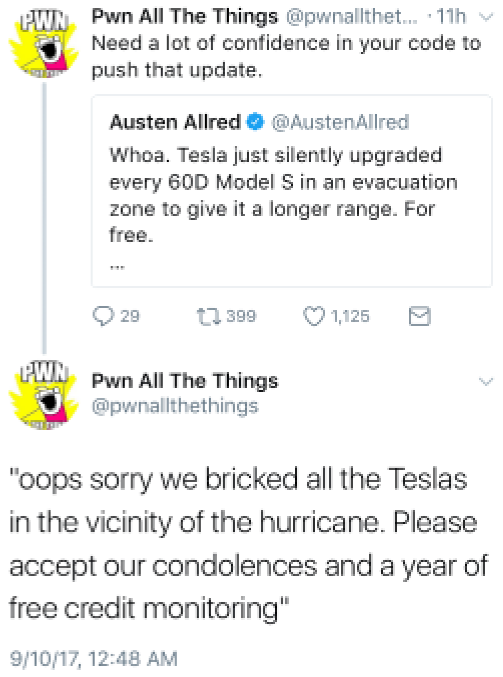
--Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (DHS)
--Wireless 'BlueBorne' impacts billions of bluetooth devices (Threat Post)
--It's September 2017, and .NET lets PDFs hijack your Windows PC (the Register)
--FireEye Uncovers CVE-2017-8759: Zero-Day Used in the Wild to Distribute FINSPY (FireEye)
--D-Link router riddled with 0-day flaws (the Register)

Network defense:

--$1mm bounty for TOR (CSO)
--Businesses Fail to Properly Secure, Assess SSH: ISACA (Dark Reading)
--Why InfoSec Hiring Managers Miss the Oasis in the Desert (Dark Reading)

(In)Secure Takes – Twitter's best from the week

September 14, 2017



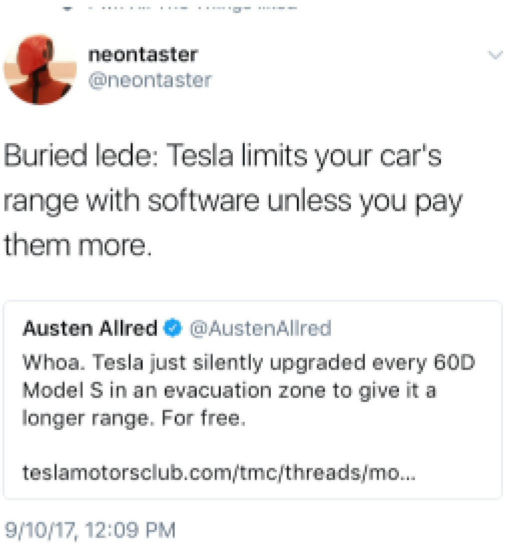
Pwn All The Things @pwnallthet... · 11h
Need a lot of confidence in your code to push that update.

> Austen Allred @AustenAllred
> Whoa. Tesla just silently upgraded every 60D Model S in an evacuation zone to give it a longer range. For free.
> ...

Pwn All The Things
@pwnallthethings

"oops sorry we bricked all the Teslas in the vicinity of the hurricane. Please accept our condolences and a year of free credit monitoring"

9/10/17, 12:48 AM



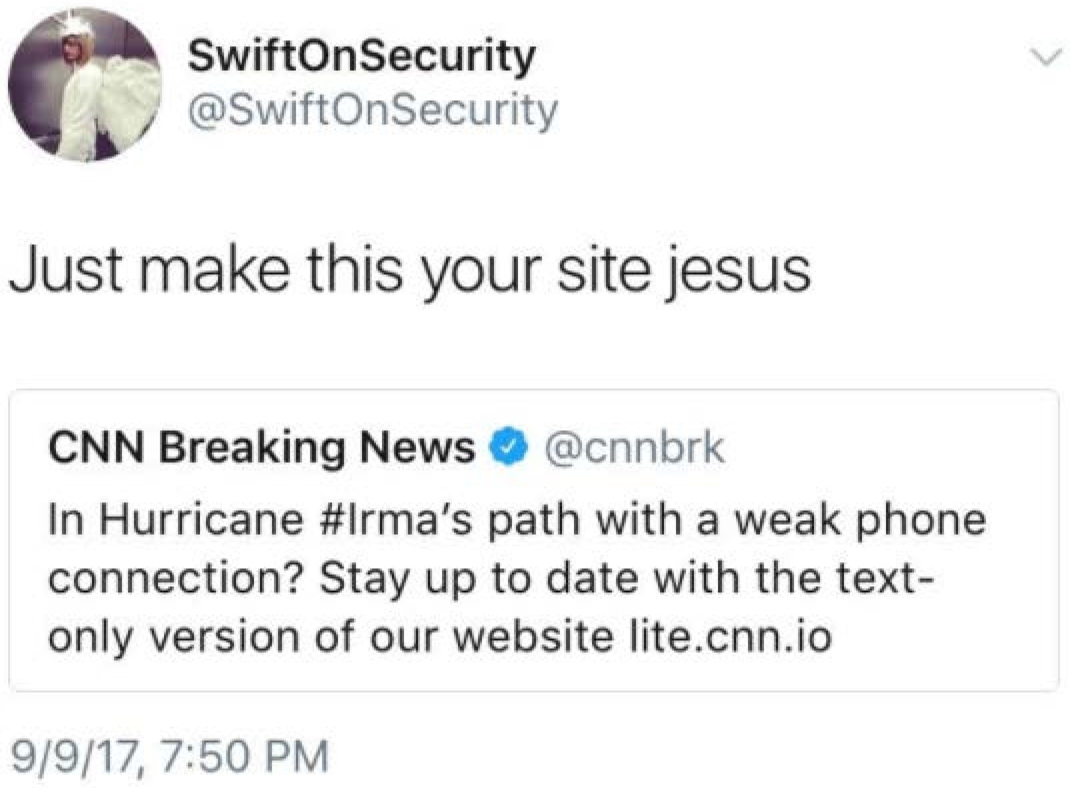
neontaster
@neontaster

Buried lede: Tesla limits your car's range with software unless you pay them more.

> Austen Allred @AustenAllred
> Whoa. Tesla just silently upgraded every 60D Model S in an evacuation zone to give it a longer range. For free.
>
> teslamotorsclub.com/tmc/threads/mo...

9/10/17, 12:09 PM

September 14, 2017

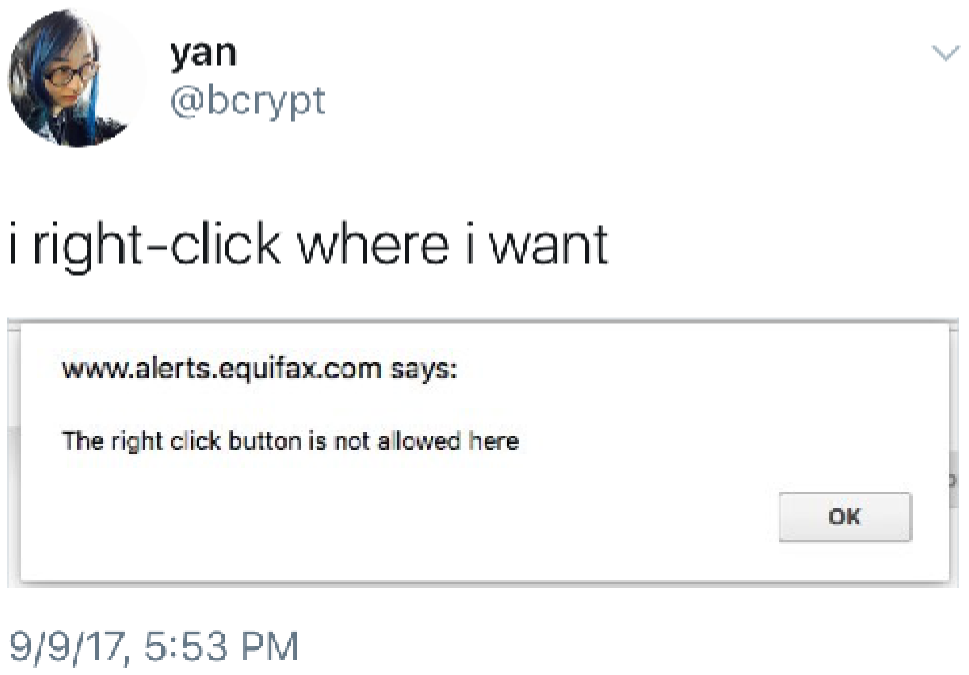


SwiftOnSecurity
@SwiftOnSecurity

Just make this your site jesus

CNN Breaking News @cnnbrk
In Hurricane #Irma's path with a weak phone connection? Stay up to date with the text-only version of our website lite.cnn.io

9/9/17, 7:50 PM



yan
@bcrypt

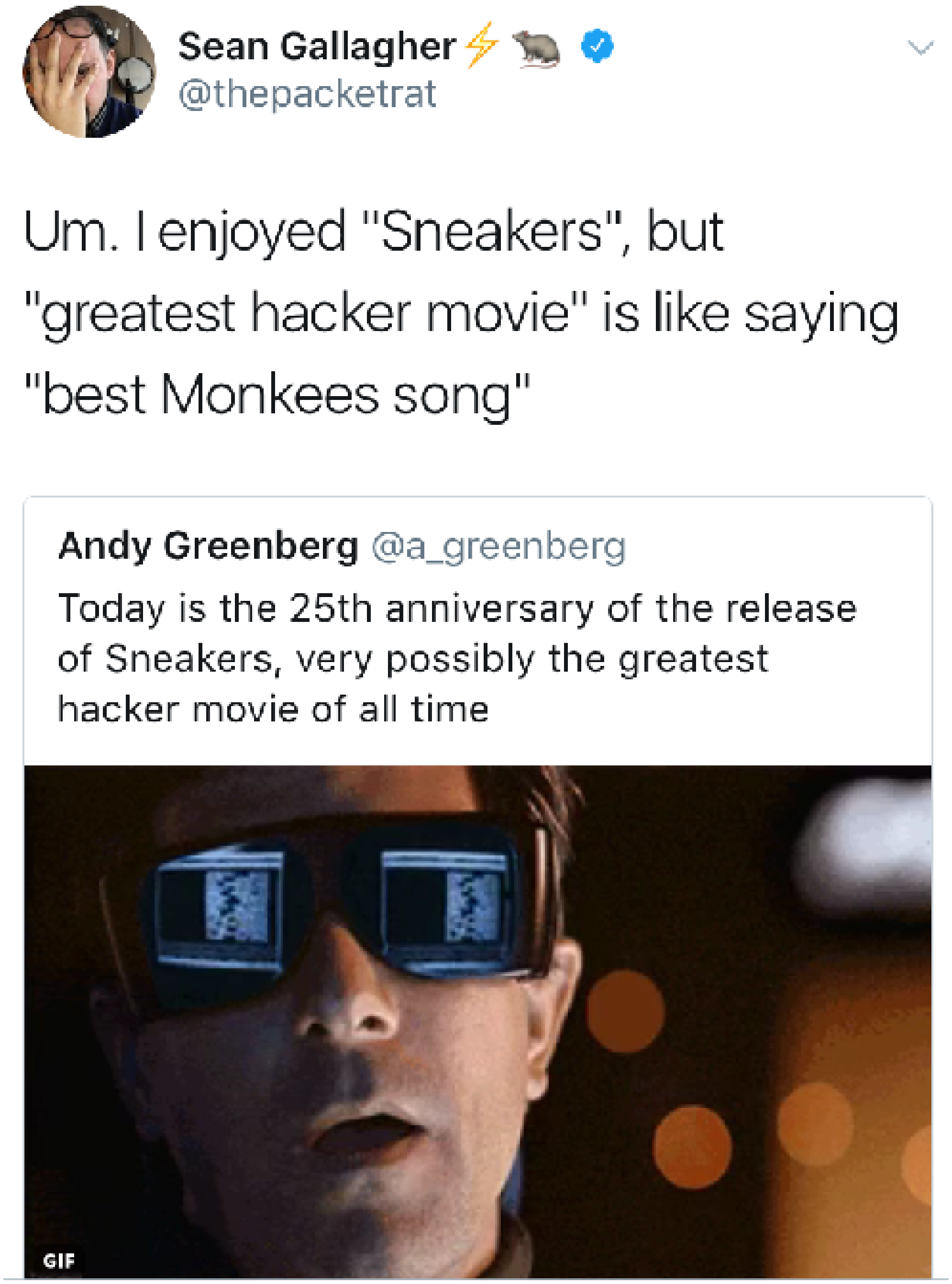
i right-click where i want

www.alerts.equifax.com says:

The right click button is not allowed here

9/9/17, 5:53 PM

September 14, 2017



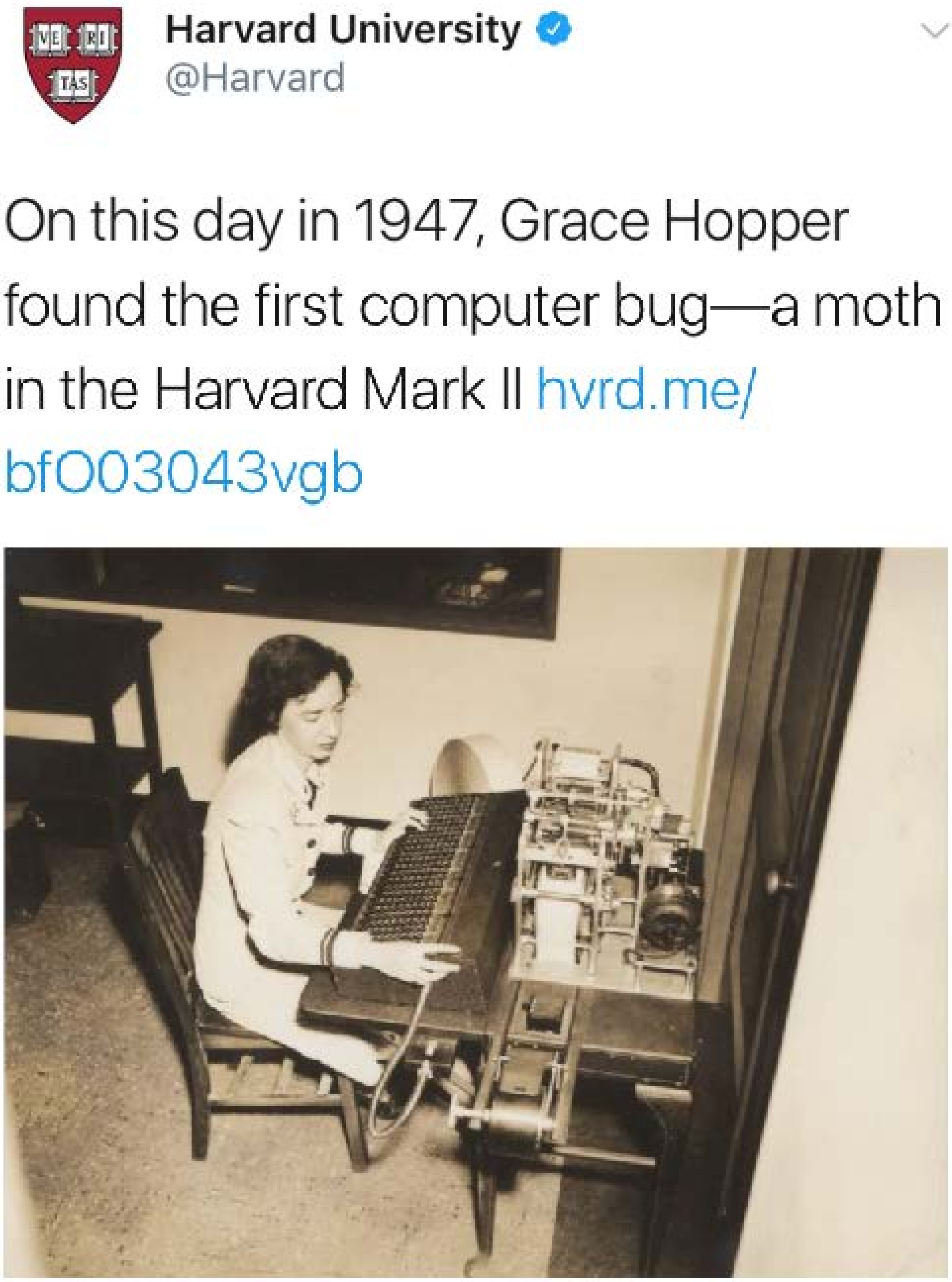
Sean Gallagher⚡🐀
@thepacketrat

Um. I enjoyed "Sneakers", but "greatest hacker movie" is like saying "best Monkees song"

Andy Greenberg @a_greenberg

Today is the 25th anniversary of the release of Sneakers, very possibly the greatest hacker movie of all time

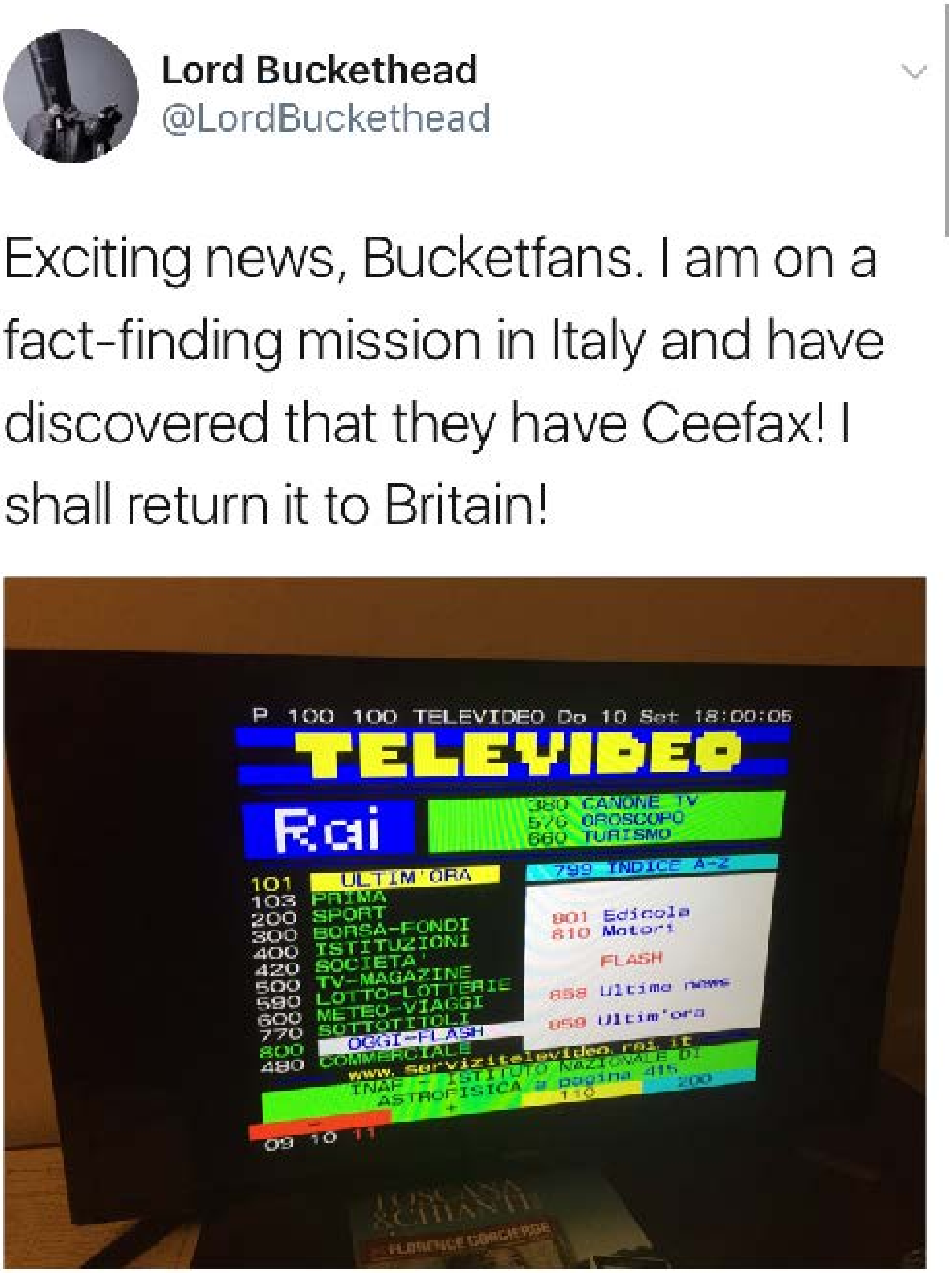
September 14, 2017



Harvard University
@Harvard

On this day in 1947, Grace Hopper found the first computer bug—a moth in the Harvard Mark II hvrd.me/bfO03043vgb

September 14, 2017



Lord Buckethead
@LordBuckethead

Exciting news, Bucketfans. I am on a fact-finding mission in Italy and have discovered that they have Ceefax! I shall return it to Britain!

Contact us: follow @NHISAC and email at bflatgard@nhisac.org