FOLEY HOAG LLP

Driving Business Advantage

The Legal Benefits and Practical Problems of Data Encryption in the Workplace (and Elsewhere)

Presentation to Union College, Department of Computer Science

March 2, 2018

COLIN J. ZICK
Foley Hoag LLP
czick@foleyhoag.com
(617) 832-1275

© 2018 Foley Hoag LLP. All Rights Reserved.

FOLEY HOAG LLP
Driving Business Advantage

Colin J. Zick

Partner, Chair, Privacy and Data Security Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.

- Advises on issues involving the transfer of data between jurisdictions, including EU-US Privacy Shield, and other relevant data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.

- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com, and was recognized by JD Supra's 2017 Readers Choice Awards. Serves as outside counsel to the Advanced Cyber Security Center, and is a member of Law360's Privacy & Consumer Protection editorial advisory board.

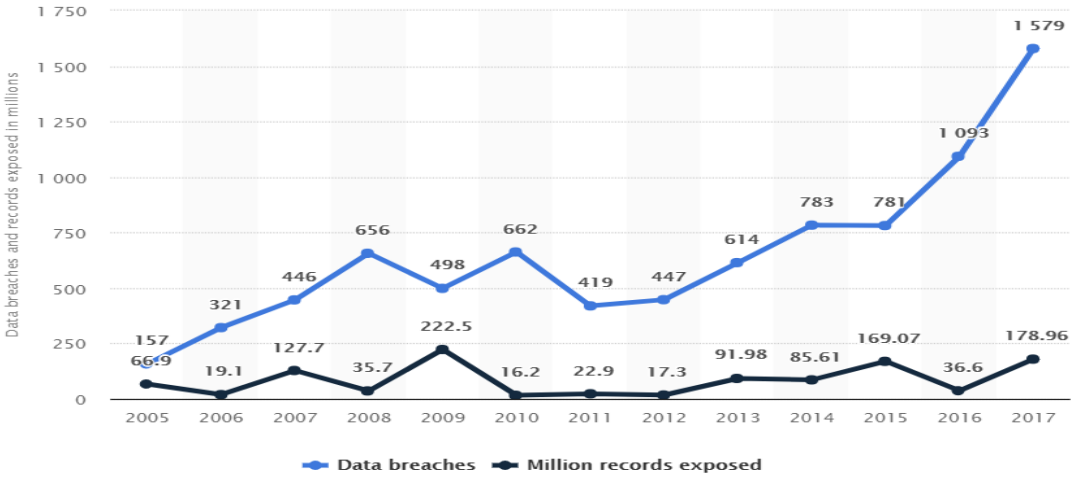
© 2018 Foley Hoag LLP. All Rights Reserved.

Data Breaches are Both Expensive and Numerous

- **Average data breach costs:**
  - 2017: US $6.7 million per breach

- **Number of breaches:**
  - In 2017, 1,579 reported breaches with nearly to 179 million records exposed.

Source: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/



© 2018 Foley Hoag LLP. All Rights Reserved.

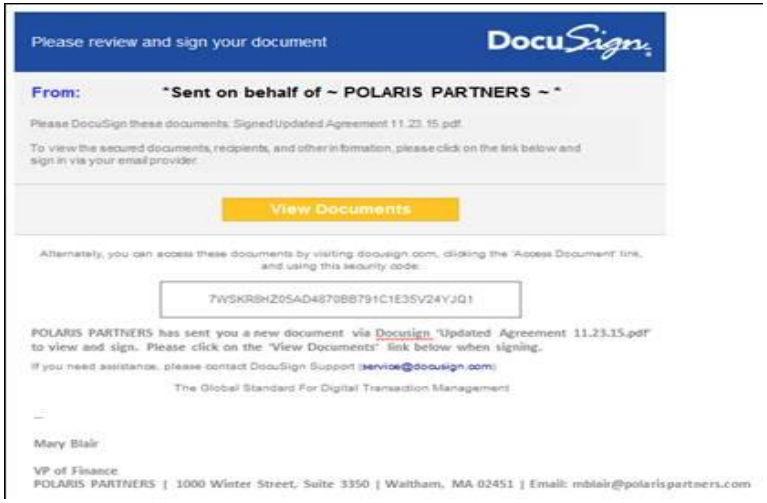
Examples of Information Security Risks - Cyber Attacks

- Spoofing and Phishing: http://www.reedsmith.com/IMPORTANT_Email_Spoof_Impersonation_Notice_01-22-2014/

> We want to make you aware of an email spoof that is impersonating the domain name of several large law firms, including Reed Smith.
>
> The spoof involves an email falsely purporting to be from Reed Smith or another large law firm, and describing a "Notice to Appear in Court" or other fictitious court appearance. If you received such an email, please be aware that it did not come from our Firm. In addition, note that the email may contain a link to a computer virus or other malware. You should not open the email or attachments, or respond to it in any way.

- Law firms are prime targets for cyber attacks

  http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms



© 2018 Foley Hoag LLP. All Rights Reserved.

Examples of Information Security Risks - Phishing

- If it looks too good to be true… don't click on it or reply to it!

From: outlook_1c94170a1a1a7502@outlook.com on behalf of Lachlan Wang <lach.wang@hotmail.com>
To:
Cc:
Subject: Legal Counsel.

Dear Counsel,
Our company is in need of a Legal Counsel who can handle litigation matters against one of our client due to breach of contract. Please contact us for more details if you are interested.
Regards,
Lachlan Wang
Director of Human Resources
Ma-Shan Iron & Steel Co. Ltd

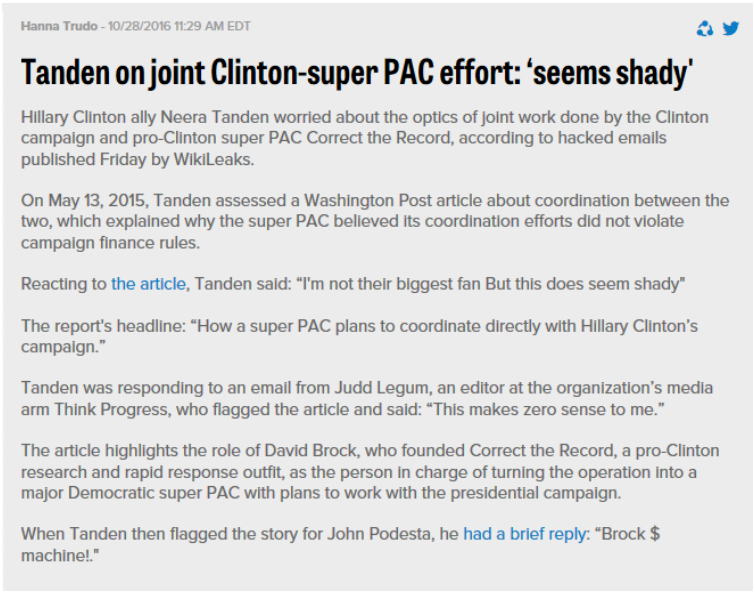
- If it requires immediate response, verify its authenticity before clicking.

> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

© 2018 Foley Hoag LLP. All Rights Reserved.

Examples of Information Security Risks – Wikileaks type email hacks

- How did Team Clinton fail?
  - Inappropriate IT vetting of phishing scam
  - Podesta failed to use two factor authentication
  - Poor virtual situational awareness



Hanna Trudo - 10/28/2016 11:29 AM EDT

Tanden on joint Clinton-super PAC effort: 'seems shady'

Hillary Clinton ally Neera Tanden worried about the optics of joint work done by the Clinton campaign and pro-Clinton super PAC Correct the Record, according to hacked emails published Friday by WikiLeaks.

On May 13, 2015, Tanden assessed a Washington Post article about coordination between the two, which explained why the super PAC believed its coordination efforts did not violate campaign finance rules.

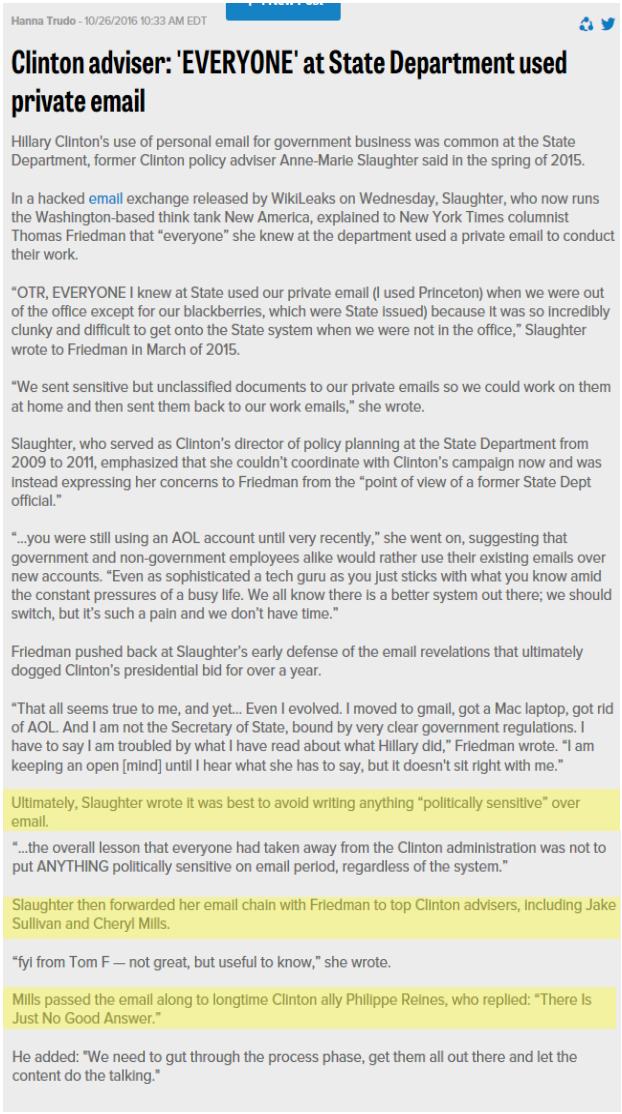
Reacting to the article, Tanden said: "I'm not their biggest fan But this does seem shady"

The report's headline: "How a super PAC plans to coordinate directly with Hillary Clinton's campaign."

Tanden was responding to an email from Judd Legum, an editor at the organization's media arm Think Progress, who flagged the article and said: "This makes zero sense to me."

The article highlights the role of David Brock, who founded Correct the Record, a pro-Clinton research and rapid response outfit, as the person in charge of turning the operation into a major Democratic super PAC with plans to work with the presidential campaign.

When Tanden then flagged the story for John Podesta, he had a brief reply: "Brock $ machine!."



Hanna Trudo - 10/26/2016 10:33 AM EDT

Clinton adviser: 'EVERYONE' at State Department used private email

Hillary Clinton's use of personal email for government business was common at the State Department, former Clinton policy adviser Anne-Marie Slaughter said in the spring of 2015.

In a hacked email exchange released by WikiLeaks on Wednesday, Slaughter, who now runs the Washington-based think tank New America, explained to New York Times columnist Thomas Friedman that "everyone" she knew at the department used a private email to conduct their work.

"OTR, EVERYONE I knew at State used our private email (I used Princeton) when we were out of the office except for our blackberries, which were State issued) because it was so incredibly clunky and difficult to get onto the State system when we were not in the office," Slaughter wrote to Friedman in March of 2015.

"We sent sensitive but unclassified documents to our private emails so we could work on them at home and then sent them back to our work emails," she wrote.

Slaughter, who served as Clinton's director of policy planning at the State Department from 2009 to 2011, emphasized that she couldn't coordinate with Clinton's campaign now and was instead expressing her concerns to Friedman from the "point of view of a former State Dept official."

"...you were still using an AOL account until very recently," she went on, suggesting that government and non-government employees alike would rather use their existing emails over new accounts. "Even as sophisticated a tech guru as you just sticks with what you know amid the constant pressures of a busy life. We all know there is a better system out there; we should switch, but it's such a pain and we don't have time."

Friedman pushed back at Slaughter's early defense of the email revelations that ultimately dogged Clinton's presidential bid for over a year.

"That all seems true to me, and yet... Even I evolved. I moved to gmail, got a Mac laptop, got rid of AOL. And I am not the Secretary of State, bound by very clear government regulations. I have to say I am troubled by what I have read about what Hillary did," Friedman wrote. "I am keeping an open [mind] until I hear what she has to say, but it doesn't sit right with me."

Ultimately, Slaughter wrote it was best to avoid writing anything "politically sensitive" over email.

"...the overall lesson that everyone had taken away from the Clinton administration was not to put ANYTHING politically sensitive on email period, regardless of the system."

Slaughter then forwarded her email chain with Friedman to top Clinton advisers, including Jake Sullivan and Cheryl Mills.

"fyi from Tom F — not great, but useful to know," she wrote.

Mills passed the email along to longtime Clinton ally Philippe Reines, who replied: "There Is Just No Good Answer."

He added: "We need to gut through the process phase, get them all out there and let the content do the talking."

© 2018 Foley Hoag LLP. All Rights Reserved.

The Law Requires Many Companies to Protect Confidences and Avoid Security Breaches

- In many states, personal information in motion must be encrypted, unless encryption is not technically feasible:
  - New York law: *NY Gen. Bus. Law § 899-aa*
  - Massachusetts law: *201 Code of Mass. Regulations 17.00 et seq.*
- Federal law is similar:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - FTC Identity Theft Red Flags Rule

© 2018 Foley Hoag LLP. All Rights Reserved.

Encryption Is an Easy Way to Limit Liability for a Breach

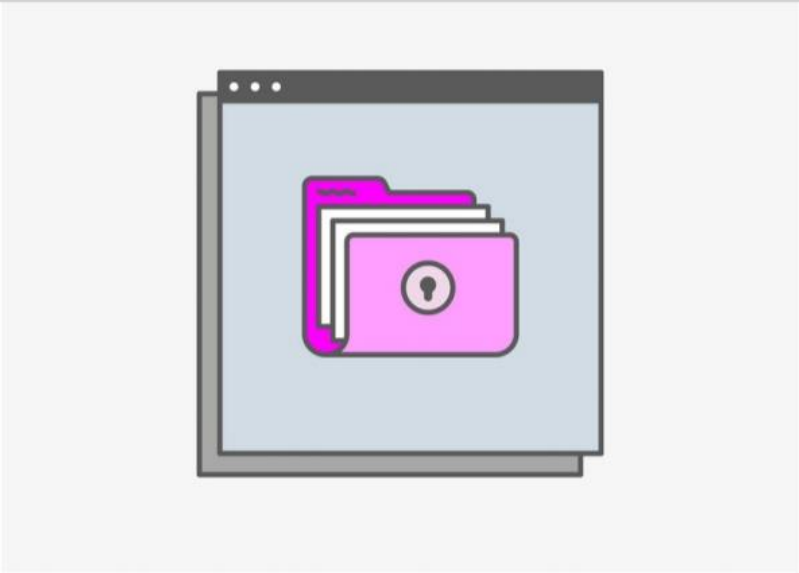
© 2018 Foley Hoag LLP. All Rights Reserved.

Encryption Is Now So Easy, Even an RPI Hockey Player Can Do It

ANDY GREENBERG SECURITY 12.09.17 06:00 AM

HOW TO ENCRYPT ALL OF THE THINGS

SUBSCRIBE



The best way to encrypt data at rest—rather than messages in motion—is en masse, by encrypting compartments of your storage, or simply encrypting your entire hard drive. AARON FERNANDEZ

CRYPTOGRAPHY WAS ONCE the realm of academics, intelligence services, and a few cypherpunk hobbyists who sought to break the monopoly on that science of secrecy. Today, the cypherpunks have won: Encryption is everywhere. It's easier to use than ever before. And no amount of handwringing over its surveillance-

Source: Wired.com

© 2018 Foley Hoag LLP. All Rights Reserved.

Survey: Massachusetts Residents Concerned Over Personal Data

- In December 2017, the Advanced Cyber Security Center announced the results of a cyber security public opinion survey that finds Massachusetts residents deeply concerned over privacy and the control of their personal data. Titled “Cyber Security Post Equifax: Perceptions and Priorities from Massachusetts Residents,” the study examines public opinion on consumer and privacy matters related to cyber security.
- Key findings include:
  - 89% of Massachusetts residents report that keeping their personal information private is a concern, with a majority saying it is a major concern.
  - While almost two thirds value the benefits of the Internet over the threats to privacy it brings, the overwhelming majority of residents (92 percent) believe the federal government should set tougher standards for technology and data companies to protect the personal data of consumers.
  - 68% say they are unlikely to continue to do business with an organization that suffers a data breach that releases personal data.
  - At the same time, many consumers are not taking actions yet themselves, with close to 50% reporting they have taken no steps to protect their personal credit information.
  - Consumers appear to lack a basic foundation of knowledge about how their data is being used and appear unaware of the tools available to them to protect their data.

Source: ACSC Advanced Cyber Security Center
Threat Sharing | Collaborative Defense | Education

© 2018 Foley Hoag LLP. All Rights Reserved.

FOLEY HOAG LLP
Driving Business Advantage

Yet Users Hate It, or Don't Understand It

Why No One Uses Encrypted Email Messages

by **Chris Hoffman** on April 30th, 2014

With so much concern about government surveillance, corporate espionage, and everyday identity theft, it may seem surprising that so few people use encrypted email messages. Try using encrypted email and you'll find it to be difficult and complicated to use.

Encrypted emails are a headache to deal with. You may be able to deal with the complexity, but the people you want to communicate with also have to handle it.

Source: Wired.com

© 2018 Foley Hoag LLP. All Rights Reserved.

Law Enforcement Hates Encryption

KEVIN POULSEN SECURITY 10.08.14 06:30 AM

APPLE'S IPHONE ENCRYPTION IS A GODSEND, EVEN IF COPS HATE IT

THEN ONE/WIRED

IT TOOK THE upheaval of the Edward Snowden revelations to make clear to everyone that we need protection from snooping, governmental and otherwise. Snowden illustrated the capabilities of determined spies, and said what security experts have preached for years: Strong encryption of our data is a basic necessity, not a luxury.

Source: Wired.com

© 2018 Foley Hoag LLP. All Rights Reserved.

FOLEY HOAG LLP
Driving Business Advantage

U.S. v. Microsoft: Will It Drive Encryption?

- U.S. Supreme Court case argued earlier this week.
- The legal question is whether Microsoft, as a United States provider of email services, must comply with a probable-cause-based warrant issued under the Stored Communications Act by making disclosure in the United States of electronic communications within Microsoft's control, even if the provider has decided to store that material abroad.
- Microsoft told the justices the SCA only applies within the United States, so the company cannot be compelled to turn over emails stored outside the country.
- The U.S. government argued that while U.S. laws don't normally apply outside its borders, the SCA focuses on "classically domestic conduct": Microsoft is simply being asked to turn over electronic records that it controls, even if those records happen to be stored elsewhere.
- And if Microsoft discloses EU-based records, it will violate EU law.

Possible application of the law of unintended consequences:
Will a decision for the U.S. government result in more widespread encryption to defeat SCA warrants?

© 2018 Foley Hoag LLP. All Rights Reserved.

FOLEY HOAG LLP
Driving Business Advantage

Google's Promoting Encryption?

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Security Through Transparency

January 12, 2017

Posted by Ryan Hurst and Gary Belvin, Security and Privacy Engineering

Encryption is a foundational technology for the web. We've spent a lot of time working through the intricacies of making encrypted apps easy to use and in the process, realized that a generic, secure way to discover a recipient's public keys for addressing messages correctly is important. Not only would such a thing be beneficial across many applications, but nothing like this exists as a generic technology.

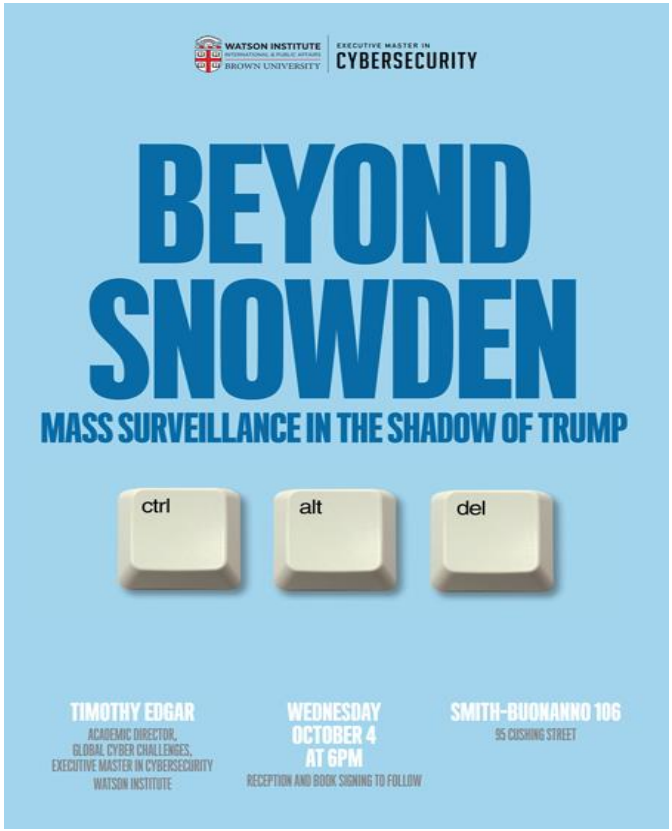
A solution would need to reliably scale to internet size while providing a way to establish secure communications through untrusted servers. It became clear that if we combined insights from Certificate Transparency and CONIKS we could build a system with the properties we wanted and more.

The result is Key Transparency, which we're making available as an open-source prototype today.

© 2018 Foley Hoag LLP. All Rights Reserved.

The EU Doesn't Trust the US Anymore: Will This Drive More Encryption?

- Schrems case: "the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security." Source: EU Communication (2013)847 on the Functioning of the Safe Harbour



© 2018 Foley Hoag LLP. All Rights Reserved.

FOLEY HOAG LLP
Driving Business Advantage

Three Emerging "Truths" about Encryption

The Electronic Frontier Foundation's Seth Schoen and Andrew Crocker see "three truths" about encryption:

- First, there is no substitute for "strong" encryption, i.e., encryption without any intentionally included method for any party (other than the intended recipient/device holder) to access plaintext to allow decryption on demand by the government.
- Second, an exceptional access mandate will help law enforcement and intelligence investigations in certain cases.
- Third, "strong" encryption cannot be successfully fully outlawed, given:
  - its proliferation
  - the fact that a large proportion of encryption systems are open-source
  - the fact that U.S. law has limited reach on the global stage.

Source: https://www.eff.org/deeplinks/2018/02/new-national-academy-sciences-report-encryption-asks-wrong-questions

© 2018 Foley Hoag LLP. All Rights Reserved.

New Ideas for Governments

- The EastWest Institute, a New York-based security think tank, has produced a report offering nine points:
  - encourages governments to allow the use of strong encryption
  - while creating a legal framework for authorized law enforcement to access the plain text of encrypted data in limited cases.

  It was presented last month at the Munich Security Conference.
- The National Academies of Science released a report on encryption calls on both sides to give and get a little:
  - Governments should accept that strong encryption is important and stop trying to undermine it.
  - Companies need to allow for legitimate government requests for access to the keys that lock that information.
    - Those requested must be limited and have to go through open judicial processes to ensure accountability.

Source: https://www.usatoday.com/story/tech/2018/02/15/encryption-we-cant-live-without-law-enforcement-cant-live/336101002/

Does this suggest a willingness for all sides to find a workable way forward on encryption, as incidents of data breach increase?

© 2018 Foley Hoag LLP. All Rights Reserved.