Beyond FBI vs. Apple: What’s Next in the Crypto Wars?
INTRODUCTION - WHO AM I?

Disclaimer: These words are my own. I do not speak for these companies.
DON’T SHIP THAT FLOPPY.
PHIL ZIMMERMAN AND PGP (1990’S)

PGP
CALEA
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (1994)
WE WON!
O RLY?

- **FREAK**: March 2015
- **LOGJAM**: May 2015
- **DROWN**: March 2016
EFF and others won in the courts, US Congress, and public opinion

BULLRUN - NSA’s effort to bypass democratic mechanisms and sabotage our security anyway (in secret.)

Hidden vulnerabilities in NIST standard

Weakening of global cryptography market to ensure people have access only to compromised methods

Many details still unknown
IN THE DIGITAL AGE, ACCESS TO AND USE OF ENCRYPTION IS AN ENABLER OF THE RIGHT TO PRIVACY.
Paris attacks / Telegram found on phones

ISIL's media org, the Al-Hayat Media Group, launched a website on the dark web, recommending Telegram.

Such activities could be used as pretext to monitor citizens and could be used to suppress dissidents.

We cannot make messaging technology secure for everyone except for criminals / terrorists.
“ENCRYPTION DOES MAKE TARGETED SURVEILLANCE MUCH HARDER. SO DOES CASH, BEARER BONDS, FAKE MUSTACHES, HATS, HAIR DYE, BLANKETS, HORSES, BOATS, AND FORESTS.”

- OLIVER DAY
  (SECURING CHANGE)
DON'T PANIC.
Making Progress on the “Going Dark” Debate
NOT JUST ONE PHONE.
63 ongoing phone-unlocking cases in US, 175 phones in NYC
Adam Khan @Khanoisseur

FBI: Give us the keys, they'll be safe with us

Apple: No they won't

FBI: Just do it what could go wrong

Apple: 

FBI quietly admits that a group called "APT6" spends years inside US government networks conducting espionage:

FBI Quietly Admits to Multi-Year APT Attack, Sensitive Data Stolen
In fact, BlackBerry has recently signalled a willingness to deal with law enforcement on encryption, with company CEO John Chen writing last year that "we reject the notion that tech companies should refuse reasonable, lawful access requests."

"That's the reality of it, that's what we don't want the general public to know."

Through the course of the trial, the defense managed to get the Crown to admit that this wasn't just a key. It was the key. This was BlackBerry's global encryption key.
ARE CRIMINALS THAT SMART?
HIDING YOURSELF ISN’T THAT EASY.

- Disable default device backups to the cloud.
- Disable default device key backups to the cloud.
- Disable default device biometric decryption (touchID).
- Avoid sending incriminating evidence by any non-encrypted means.
- Disable default cloud storage for each app.
- Don’t call or text anyone (leaving behind metadata)
Where Can You Encrypt?

At least 6 countries in Europe and Asia have already addressed WhatsApp-style encryption

- Laws against it already
- Proposed legislation would penalize it
- Government formally supports it

Source: vocativ
Mass Surveillance, A Growing Trend

Mass Surveillance

Privacy
MASS SURVEILLANCE BY COUNTRY

- Worst
  - China
  - Malaysia
  - Russia

- Slightly Better
  - Singapore
  - UK

- Meh.
  - Taiwan
  - Thailand
  - United States.

- Best
  - Greece, which was judged to have 'adequate safeguards against abuse'

Source: Privacy International 2007
(TS//SI//REL) Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?

(TS//SI//REL) Twenty years ago, the fact that communications were encrypted meant they were very likely to contain foreign intelligence, because only governments or other important targets had the resources to purchase or develop and implement encrypted communications. Today, anyone who uses the Internet can access web pages via the strong commercial encryption provided by HTTPS, and companies of all sizes can implement virtual private networks (VPN) to permit their employees to access sensitive or proprietary company data securely via an Internet connection from anywhere in the world. SID refers to this widespread encryption, which poses great challenges to SIGINT, as "ubiquitous encryption."
ENCRYPT
ALL THE THINGS!
WHERE ARE WE GOING?

- Expect companies to introduce additional encryption in products. Apple is well on their way with secure enclaves in their hardware.
- Expect governments to attempt to introduce legislation banning strong encryption and promoting impossible backdoors.
- Oh wait, they already have...
‘A GOVERNMENT THAT SPIES ON ITS CITIZENS. WHAT’S NOT TO LIKE?’

President Putin is a big fan of Britain’s surveillance laws and Russian authorities regularly use them to justify their own snooping. So we think he’s going to love the new Investigatory Powers Bill going through the UK Parliament right now. By allowing the bulk collection of everyone’s phone and internet history, it will place the whole population under surveillance. If, unlike Mr Putin, you feel that mass surveillance is a step too far then take action before it’s too late at dontspyonus.org.uk #DontSpyOnUs #IPBill

‘WELL DONE, BRITAIN! NO ONE MONITORS THEIR PEOPLE QUITE LIKE YOU’

The Investigatory Powers Bill, going through the UK Parliament right now, will make the UK a world leader in surveillance and the envy of people like China’s President Xi Jinping. By allowing the bulk collection and analysis of everyone’s phone and internet history this Bill will automatically put us all under surveillance, without any suspicion of wrongdoing. If, unlike Xi Jinping, you feel that mass surveillance is a step too far then take action before it’s too late at dontspyonus.org.uk #DontSpyOnUs #IPBill
UK CALLS FOR OUTLAWING NON-BACKDOORED CRYPTO (2015)

- Prime minister David Cameron, Jan. 2015 calls for ban on end-to-end encryption that the government cannot read.
- If you can’t say something to a friend or family member without the fear the government, your neighbor or your boss will overhear, your free expression is deeply curtailed.
- There is no such thing as “good guy encryption” and “bad guy encryption”.

SNOOPER’S CHARTER
“Snooper’s Charter”

“maintain records of each user's internet browsing activity (including social media), email correspondence, voice calls, internet gaming, and mobile phone messaging services and store the records for 12 months. Retention of email and telephone contact data for this time is already required by the Data Retention Regulations 2014.”

The anticipated cost is £1.8 billion.

UK Home Secretary Theresa May
Ridiculous.

Privacy advocates who expected the worst weren’t disappointed.

Make all of our online data "intelligible" when presented with a court order.

The bill defines intelligible as "decrypted, deciphered, decoded, demodulated, or deobfuscated"

As currently written, the draft likely even outlaws forward secrecy. (source: EFF - More on this in a second.)
The Netherlands government issued a strong statement on Monday against weakening encryption for the purposes of law enforcement and intelligence agencies.
Nearly one in two Internet users say privacy and security concerns have now stopped them from doing basic things online — such as posting to social networks, expressing opinions in forums or even buying things from websites, according to a new government survey released Friday.
WHAT CAN YOU DO?
WHAT CAN YOU DO?

IN CHARGE OF HTTP-BASED SERVERS AND SERVICES? (OR VPN?)

- Implement proper, always-on HTTPS - you have no excuse!
- Enable HPKP (pinning for TLS certificates)
- Enable HSTS (always talk to me in HTTPS)
- Enable PFS (Perfect forward secrecy)
- Verify your implementation (https://www.ssllabs.com)
- If possible, ask to be added to the HSTS preload list (chrome)
WHAT CAN YOU DO?

THIS ISN’T HARD, IT’S NEARLY FREE NOW.

LET’S ENCRYPT

https://letsencrypt.org/

MOZILLA RECOMMENDED CIPHER SUITES

https://mozilla.github.io/server-side-tls/ssl-config-generator/
LET’S ENCRYPT

MAKING GOOD PROGRESS – LET’S ENCRYPT
WHAT CAN YOU DO?

ARE YOU A DEVELOPER?

- Encrypt data at Rest and in Transit, even inside your company’s network.
  - Please don’t reinvent the “secure messaging” wheel.
    - It’s been done too many times.
    - You’re probably (not) a cryptographer.
    - Signal is doing it better than you anyway.
WHAT CAN YOU DO?

END-USER

- Know your vulnerabilities and threat model
- Promote end-to-end, encryption-by-default on projects that you work on
- Encrypt your phone, text messages (Signal), and hard disk
- Use strong passwords with a password manager and promote the use of 2-factor in your organization
- Use Tor.
- Enable and install HTTPS Everywhere, Adblockers, uBlock, etc.
WHAT CAN YOU DO?

POLITICALLY . . .

- Demand that your representatives in government block anti-encryption bills

- Help the EFF, ACLU, and other privacy-promoting organizations with your donations and time.

- We can fight with technology, but fighting them with legislation and precedent cases will probably be more effective in the long-run.

- Let’s all work together to make the Internet more secure.
THANK YOU!

JOHN ADAMS — @NETIK