

# *Quantifying Law Enforcement's "Going Dark" Problem:*

## *Statistics Collection Tool*

---

January 27, 2017

# “Going Dark”

---

## Strategic Gap

- As a result of the fundamental shift in communications services and technologies, criminal and national security investigations are unable to obtain needed evidence and intelligence despite having the legal authority to do so

## Impediments

- We continue to lose ground to rapidly-changing global communications services and technologies
- Public disclosures have created an environment that makes even the discussion of new lawful intercept legislation very difficult and provider cooperation tenuous
- Regulatory process is not timely and judicial process unproductive
- Stakeholders in legislative process have different equities
- Industry is very organized and proactive in its opposition to the development of new capabilities and legislation

# Encrypted Communications Applications

Modern communication applications have begun to implement encryption on data in motion, resulting in law enforcement's inability to access the plain text of data in transit (intercepted)

NOVEMBER 18, 2014

## WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users



On Tuesday, Whatsapp announced that it's implementing end-to-end encryption, an upgrade to its privacy protections that makes it nearly impossible for anyone to read users' messages—even the company itself.

The result is practically uncrackable encryption for hundreds of millions of phones and tablets that have Whatsapp installed—by some measures the world's largest-ever implementation of this standard of encryption in a messaging service.

W  
I  
R  
E  
D

# Challenges with Record Requests

---

The lack of a mandate on the retention of communications metadata or content and the increasing globalization of communication services have greatly complicated law enforcement's ability to obtain information on historical communications

---

On July 14, 2016, the Second Circuit Court of Appeals ruled against the United States Government in the case *Microsoft v. United States*, holding that the government cannot compel Microsoft, or other companies, to turn over the contents of customer emails stored on servers outside the United States with a warrant

**United States Court of Appeals  
FOR THE SECOND CIRCUIT**

August Term, 2015

Argued: September 9, 2015      Decided: July 14, 2016

Docket No. 14-2985

In the Matter of a Warrant to Search a Certain E-Mail  
Account Controlled and Maintained by Microsoft  
Corporation

# Device-Based Encryption

---

Communication devices have begun to deploy encryption on stored data, resulting in law enforcement's inability to access the plain text of data stored on a device or system (or cloud)

---

As of September 2016, Apple has estimated that 97% of all Apple devices are running iOS 8 or newer

Source:

<https://developer.apple.com/support/app-store>



**This means that law enforcement is unable to access the data on 97% of all password protected Apple devices**

- Law enforcement agencies do not have the ability to independently decrypt Apple devices running iOS 8, 9, or 10, irrespective of circumstance
- While some data may be uploaded to iCloud and be accessible pursuant to a search warrant, **it is unlikely that criminals will upload evidence of their crimes to iCloud**
- Smartphone encryption thus keeps digital evidence beyond the reach of law enforcement agencies, making it difficult to assist victims of crimes and to build cases against perpetrators

# Move to Encrypted Devices

In September 2014, **Apple** engineered its new mobile operating system, iOS 8, so that it can no longer assist law enforcement with search warrants written for locked devices.



**Google**, maker of the Android operating system, quickly announced plans to follow suit.



Apple and Google's operating systems run a combined **96.7% of smartphones** worldwide.

Source: <https://www.apple.com/privacy/government-information-requests>

Source: <http://officialandroid.blogspot.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html>

Source: <http://www.idc.com/proserv/smartphone-os-market-share.jsp>



## What we're most commonly asked for and how we respond.

The most common requests we receive for information come from law enforcement in the form of either a Device Request or an Account Request. Our legal team carefully reviews each request, ensuring it is accompanied by valid legal process. All content requests require a search warrant. Only a small fraction of requests from law enforcement seek content such as emails, photos, and other content stored on users' iCloud or iTunes account. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category altogether.

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Source: <https://www.apple.com/privacy/government-information-requests>

# Critical Capabilities, Targeted Use

---

## This is not an issue of mass data collection:

Apple estimates that **less than 0.00612%** of customers had data disclosed due to government information requests.

These are targeted requests for information supported by a neutral judge's determination of probable cause.

Additionally, the majority of requests Apple receives from law enforcement are on behalf of a customer who has reported a stolen device.

*Source: <http://www.apple.com/privacy/government-information-requests>*

# Quantifying the Problem

---

## Quantifying Law Enforcement's "Going Dark" Problem: We Need Your Help

A State and Local Statistical Collection Working Group is leading an effort to develop and deploy a **Statistics Collection Tool** to better quantify the full impact "Going Dark" has on investigations and cases

- The National Domestic Communications Assistance Center (NDCAC) is actively supporting the law enforcement community's efforts to quantify and address the challenges referred to as "Going Dark"

Statistics and examples are a critical part of our ongoing public policy process, and essential in our efforts to better inform public officials, citizens, and members of the media

### This Tool will:

- Give us a better idea of the national scope of the problem
- Allow us to see cases where encryption and other "Going Dark" challenges have either stopped the investigation or is limiting the ability to fully investigate



# Using the Statistics Collection Tool

---

## How to Start Using the Statistics Collection Tool

- Step 1:** To start using the tool, designate a staff member from your agency to serve as a point of contact and to input case information. That designee should contact the NDCAC Technical Resource Group at (855) 306-3222, or via email at [AskNDCAC@ic.fbi.gov](mailto:AskNDCAC@ic.fbi.gov)
- Step 2:** Your designee should also provide your contact information to the NDCAC
- Step 3:** Begin inputting the requested information either by using NDCAC's web portal or by completing a spreadsheet to submit cases in bulk, available upon request
- Step 4:** Once data is provided, you will have access to your agency's information

# Data Entry

**Home**


**Going Dark Submissions**

- Case Examples
- Device Forensics
- Records Request
- WireTap

**Generate a CALEA Worksheet**

**LETf Application**

**Videos**

 EDIT LINKS

**UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE**


## Device Forensics


Title \*

Agency Type \*

Agency Name \*

Case Number \*

Case Open  

Case Close  

Type of Case \*

- Arson
- Assault (Aggravated, Simple, Intimidation)
- Bad Checks
- Bribery
- Burglary/Breaking and Entering

POC Name (Last, First) \*

POC Phone (###.###.####) \*

POC Email \*

Case Status \*

Device Type \*

Device Manufacturer \*



What is the NDCAC?



# The NDCAC

- A national center established under the Department of Justice to leverage and share the collective technical knowledge and resources of the law enforcement community on issues involving real-time and stored communications and to strengthen law enforcement's relationship with industry
- Opened in March 2013
- One-of-a-kind assistance center designed to focus on law enforcement's challenges with communication services, training, and coordination needs
- Staffed by a diverse group of technical experts

# NDCAC and State and Local Law Enforcement Partnership



The NDCAC Advisory Board has a State and local law enforcement majority and plays critical role in setting the overall direction of the NDCAC



NDCAC's knowledge base and ability to serve as an assistance center is primarily based on collaboration among Federal, State, and local law enforcement, including

- NDCAC and Law Enforcement Subject Matter Experts
- Law enforcement requests



# NDCAC – Expanding Your Toolbox

The NDCAC is structured to provide the law enforcement community support not centrally available elsewhere. Resources include:



**Training** – *Develop and make available courses on tools, methods, and techniques pertaining to real-time and stored electronic communications*

**Technology Sharing** – *Identify and leverage innovative and effective technical solutions to share with law enforcement*



**Technical Resource Group** – *Support service that provides assistance and technical referrals to law enforcement clients*

**Law Enforcement Secure Website** – *Online access to a variety of technical products and services, register for training, and access point of contact information for law enforcement agencies and industry*



# Summary

---

- “Going Dark” presents a significant challenge to law enforcement
  - The Statistics Collection Tool will help the law enforcement community better quantify the full impact “Going Dark” has on our investigations and cases
  - Law enforcement input and support is essential to gathering valuable information that will highlight this challenge
  - The National Domestic Communications Assistance Center (NDCAC) is actively supporting the law enforcement community’s efforts to quantify and address the challenges referred to as “Going Dark”
- The NDCAC was founded to assist law enforcement overcome technical challenges
  - Lawfully-authorized electronic surveillance capabilities
  - Evidence collection on communications devices
  - Technical location capabilities

# *Additional Viewgraphs*



# San Bernardino

On Tuesday, February 16, 2016, a U.S. magistrate judge in California ordered Apple to help the FBI gain access to the phone of one of the shooters in the San Bernardino terrorist attack.

---

Apple CEO Tim Cook responded with a 1,100-word open letter to customers vowing to fight the order and defending the company's unilateral decision to encrypt all devices.



# Smart Phone Encryption Impact

On Thursday, February 18, 2016, District Attorney Vance and NYPD Commissioner Bill Bratton noted the impact of smartphone encryption on local law enforcement across the country.



Source: Jefferson Siegel/New York Daily News

- “Decisions about who can access key evidence in criminal investigations should be made by courts and legislatures, not by Apple and Google.”
- “Local law enforcement agencies around the country are grappling with the same problem of explaining to crime victims and surviving family members that we have hit an investigative roadblock or dead end, because Apple and Google no longer comply with warrants issued by judges.”
- “Apple and Google have created the first warrant-proof consumer products in American history, and the result is that crimes are going unsolved and victims are being left beyond the protection of the law.”

# A Global Challenge

In August 2015, District Attorney Vance, Paris Chief Prosecutor François Molins, City of London Police Commissioner Adrian Leppard, and Chief Prosecutor of the High Court of Spain Javier Zaragoza authored a joint op-ed for the *New York Times*.

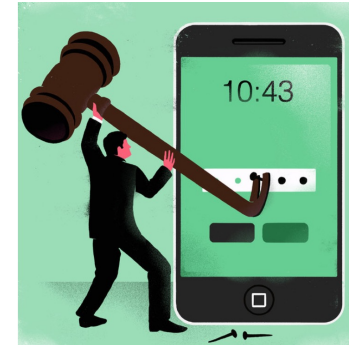
## The New York Times

[The Opinion Pages](#) | Op-Ed Contributors

### When Phone Encryption Blocks Justice

By CYRUS R. VANCE Jr., FRANÇOIS MOLINS, ADRIAN LEPPARD and JAVIER ZARAGOZA

AUG. 11, 2015



... In the United States, Britain, France, Spain and other democratic societies, the legal system gives local law enforcement agencies access to places where criminals hide evidence, including their homes, car trunks, storage facilities, computers and digital networks. Carved into the bedrock of each of these laws is a balance between the privacy rights of individuals and the public safety rights of their communities. ... It is this workable balance that proscribes the operations of local law enforcement in our cities, and guides our residents in developing their expectations of privacy. But in the absence of laws that keep pace with technology, we have enabled two Silicon Valley technology companies to upset that balance fundamentally. ...

... Full-disk encryption significantly limits our capacity to investigate these crimes and severely undermines our efficiency in the fight against terrorism. Why should we permit criminal activity to thrive in a medium unavailable to law enforcement? To investigate these cases without smartphone data is to proceed with one hand tied behind our backs.

The new encryption policies of Apple and Google have made it harder to protect people from crime. We support the privacy rights of individuals. But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. The safety of our communities depends on it.

# Misunderstood Law Enforcement Needs

In December 2015, District Attorney Vance authored an op-ed in *The Washington Post* articulating the desire to find a reasonable solution and looking to dispel certain myths about law enforcement's position on smartphone encryption.

## The Washington Post

In Theory | Opinion

### 5 ways tech companies distort the encryption debate

By Cyrus Vance Jr. December 15, 2015

*Cyrus R. Vance Jr. is the Manhattan district attorney.*



New smartphone technology is rendering our laws insufficient to protect public safety.

Last year, Apple and Google, whose software runs 96.7 percent of the world's smartphones, announced they had re-engineered their operating systems with “full-disk” encryption — expressly so that they could no longer unlock their own products. In effect, the companies are now able to say: “We will no longer comply with judges’ orders to unlock passcode-protected phones, because we no longer *can*.”

The Manhattan District Attorney's office immediately and repeatedly engaged the companies, Congress and the public in a dialogue about how this new level of encryption inhibits the investigation and prosecution of everyday crimes. ... In a recently published report, my office — in consultation with cryptologists, technologists and law enforcement partners — has proposed a solution that we believe is both technologically *and* politically feasible: Keep the operating systems of smartphones encrypted, but still answerable to locally issued search warrants. ...

MYTH 1: We want to ban encryption.

MYTH 2: We want to weaken smartphone security.

MYTH 3: We want a backdoor.

MYTH 4: We want “surveillance” of smartphone communications.

MYTH 5: We want warrantless searches.