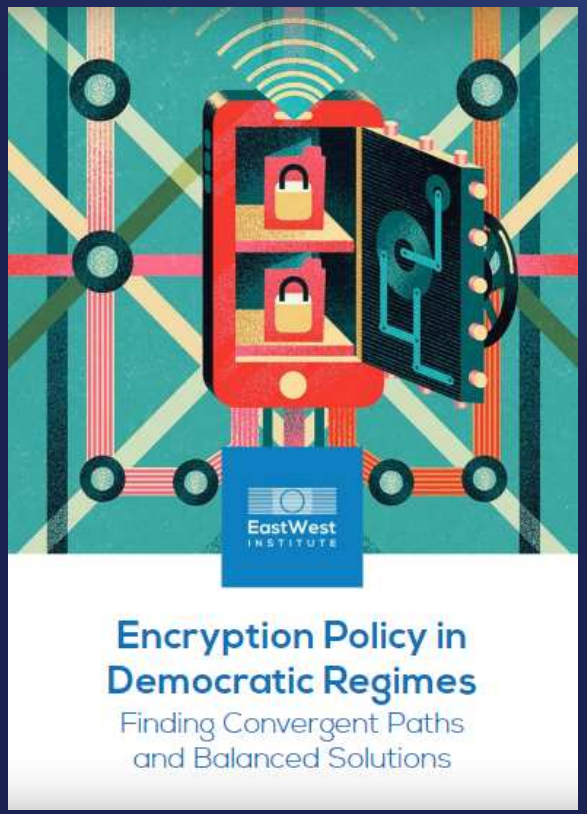
ENCRYPTION

and the IMPACT ON LAW ENFORCEMENT

New York County District Attorney's Office
Presentation to NDCAC Executive Advisory Board

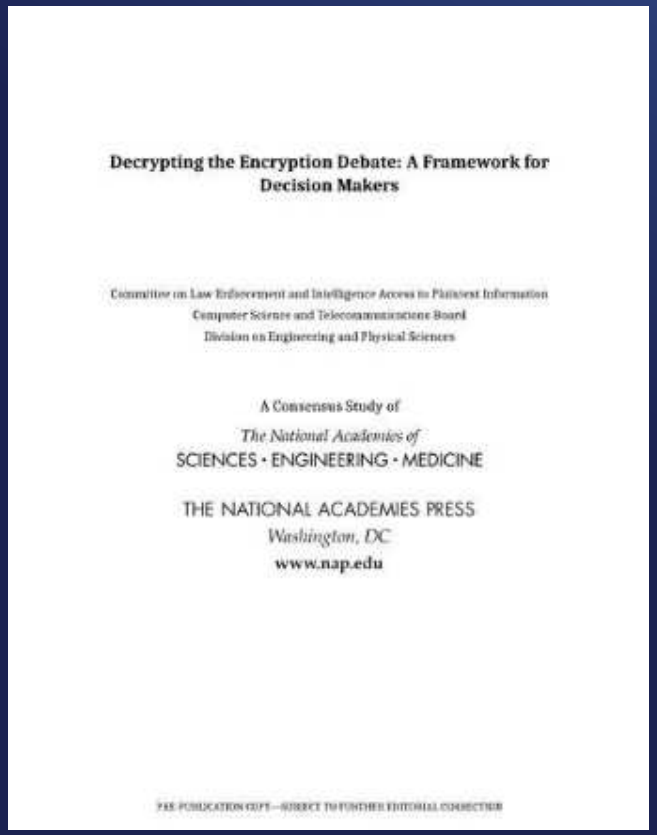
April 11, 2018

National Academy of Sciences & EastWest Institute Reports



- In February 2018, the National Academy of Sciences and East West Institute both issued new reports on the issue of encryption
- The reports discuss privacy and security implications and note that the two interests are not mutually exclusive
- Both publications address the benefits of increased discussion and the need to forge a path forward, past the "technology vs. law enforcement" dichotomy

National Academy of Sciences Report



Decrypting the Encryption Debate: A Framework for Decision Makers

Committee on Law Enforcement and Intelligence Access to Plaintext Information
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

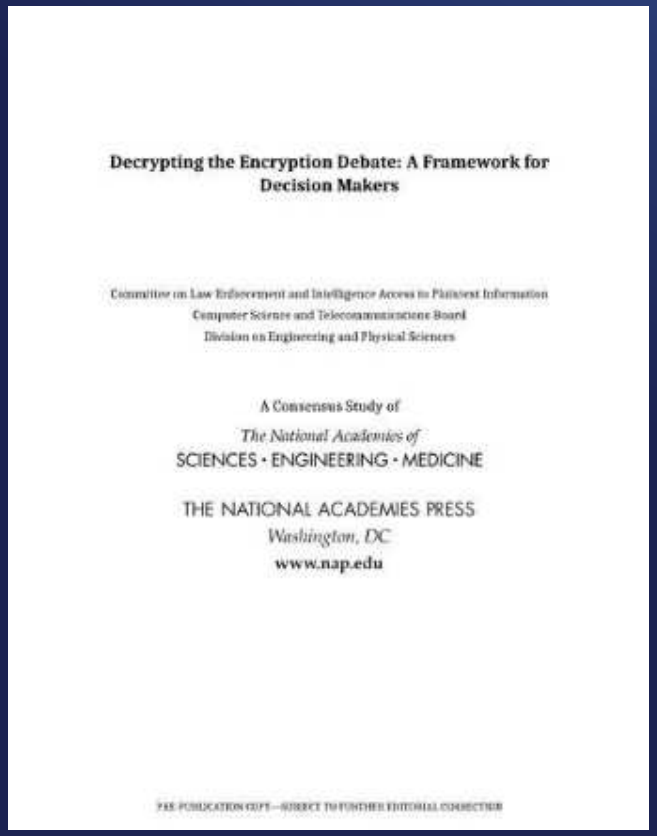
A Consensus Study of
The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

PRE-PUBLICATION COPY—SUBJECT TO FURTHER EDITORIAL CORRECTION

- 18-month study of the encryption debate
- Committee on Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption:
  - 14 members from academia, technology companies, think tanks, consultants, and law enforcement
  - Tech community representation: Google, Microsoft, Intel
  - Law enforcement representative: Richard Littlehale, Tennessee Bureau of Investigation
  - Chair: Fred H. Cate, law professor and Senior Fellow, Center for Applied Cybersecurity Research, Indiana University

National Academy of Sciences Report



Decrypting the Encryption Debate: A Framework for Decision Makers

Committee on Law Enforcement and Intelligence Access to Plaintext Information
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

A Consensus Study of
The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

PRE-PUBLICATION COPY—SUBJECT TO FURTHER EDITORIAL CORRECTION

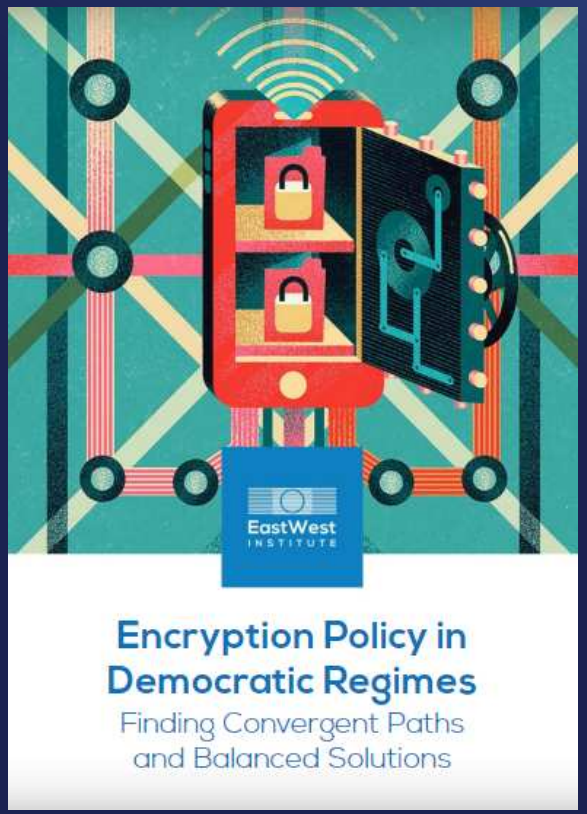
- Highlights technologists ongoing work to develop a device-based solution:
  - Ray Ozzie, Microsoft, former chief software architect
  - Stefan Savage, University of California San Diego, computer science professor
  - Ernie Brickell, Intel, former chief security officer
- Describes tradeoffs of law enforcement access to encrypted content in the current technological landscape
- Provides an eight-question framework for policymakers to consider, with the objective of maximizing effectiveness while minimizing risks
- Our hope is that this report and the framework it presents will cut through the rhetoric, inform decision-makers, and help enable an open, frank conversation about the best path forward."

  - Fred Cate, Committee Chair

National Academy of Sciences Report: Evaluation Framework

1. To what extent will the proposed approach be effective in permitting law enforcement and/or the intelligence community to access plaintext at or near the scale, timeliness, and reliability that proponents seek?
2. To what extent will the proposed approach affect the security of the type of fate or device to which access would be required, as well as cybersecurity more broadly?
3. To what extent will the proposed approach affect the privacy, civil liberties, and human rights of the targeted individuals and groups?
4. To what extent will the proposed approach affect commerce, economic competitiveness, and innovation?
5. To what extent will financial costs be imposed by the proposed approach, and who will bear them?
6. To what extent is the proposed approach consistent with existing law and other government priorities?
7. To what extent will the international context affect the proposed approach, and what will be the impact of the proposed approach internationally?
8. To what extent will the proposed approach be subject to effective ongoing evaluation and oversight?

EastWest Institute Report



- Report created in light of the current "acrimonious" nature of the discussion and entrenched stances
- Advised by EWI Encryption Breakthrough Group
  - Representation from technology sector, law enforcement, privacy advocates
  - Contributors spanning the United States, Europe, and India
- "Encryption provides great benefits and presents challenges, but most stakeholders share common interests in safety and security"

  -Bruce McConnell, EWI Global Vice President
- "Arguments are frequently made that safeguarding information privacy and security are irreconcilable challenges, but they can be complementary"

  - J. Michael Daniel, President and CEO at Cyber Threat Alliance

EastWest Institute Report: Common Interests Frame the Debate

1. Cybersecurity
   - Security of digital information
   - Confidentiality, integrity, availability
   - Increase trust in transactions and data security

2. Law Enforcement and Public Safety
   - Law enforcement access to digital information
   - Crime prevention, detection, investigation prosecution
   - Also holds an interest in cybersecurity

3. Commerce
   - Encourage innovation and efficiency
   - Market-led policies for stronger and user-friendly encryption
   - Benefit of little limitation on country of origin

4. Privacy and Other Human Rights
   - Protect citizens and dissidents from power of authoritarian regimes
   - Encryption as a tool to protect human rights, right to privacy, and freedom of opinion and expression

EastWest Institute Report: Principles

1. Balance Principle: important to find balanced solutions
2. Do-No-Harm Principle: minimize adverse effects and unintended consequences
3. Proportionality Principle: proportion of adverse effects to anticipated gains should be weighed
4. Transparency Principle: greater transparency will increase accountability and public trust
5. Holistic Approach Principle: recognize that encryption is not the only concern for law enforcement
6. Forbearance Principle: need for debate about balanced limits and standards on harnessing new collection approaches
7. Culture Principle: take into account differing cultural values and existing laws

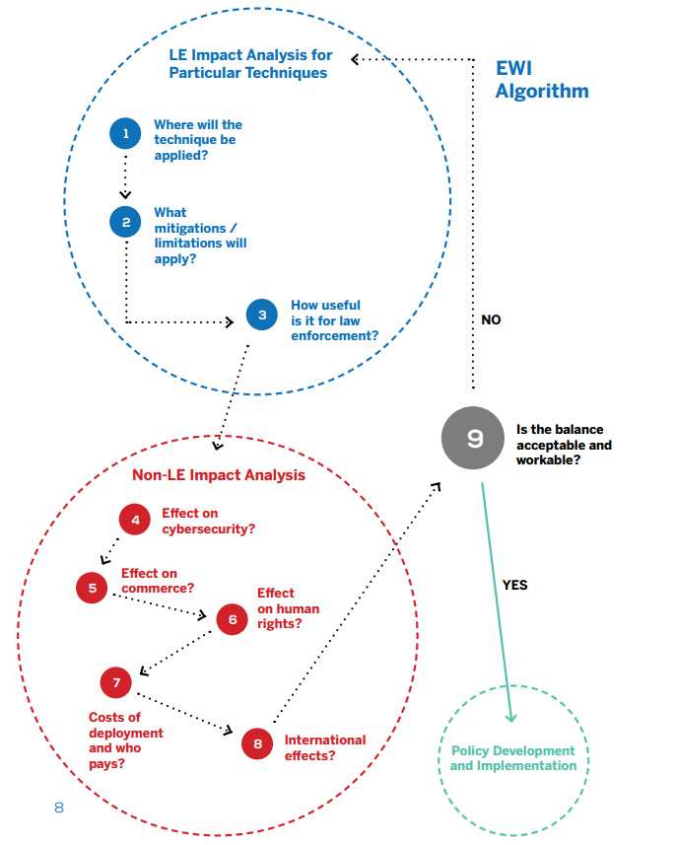
EastWest Institute Report: Assumptions

1. No single solution will solve all problems.
2. Without enacted policy, law enforcement will continue to innovate and seek plaintext.
3. Democratic regimes can devise effective encryption policies that reduce risk of abuse while providing access to law enforcement in some cases (but not risk-free or costless).
4. Human rights cannot be protected if law enforcement is ineffective.
5. Encryption is a serious practical barrier to law enforcement's ability to investigate crimes.
6. Role of encryption in data protection will increase.
7. With Internet of Things, there are increasing data streams available as potential sources of information for law enforcement, but plaintext remains essential.
8. Encryption is not the only barrier, as data may be in unfamiliar formats, outside jurisdiction, or ephemeral.
9. Any technical means that provide lawful access increases risk that criminals will exploit these means.
10. ICT product and service provers should be treated more like telecommunications companies than traditional manufacturers in the security context.
11. Giving law enforcement unrestricted lawful access may lead to abuse.
12. National encryption policies have international ramifications.

EastWest Institute Report

	Regime 1: Lawful Hacking			Regime 2: Design Mandates		
	Data at rest		Data in transit	Data at rest		Data in transit
	Data stored in cloud	Data stored on end device	Commu-nications	Data stored in cloud	Data stored on end device	Commu-nications
Approaches						
Compelled Provider Assistance	●	●	●	●	●	●
Lawful Hacking	●	●	●	Does Not Apply		
Design Mandates	Does Not Apply			●	●	●
Systemic Improvements						
Capacity Building for Law Enforcement (LE)	**Applicable to All Regimes**					
Streamline the MLAT Process						
Enhance LE/Private Sector & International LE Cooperation						

EastWest Institute Report



- Proposes 2 regimes that could enable law enforcement to access encrypted data in limited, legally-authorized cases:
  - "Lawful Hacking"
  - "Design Mandates"

- Provides 9 recommendations for policymakers:
  1. Strong Cybersecurity
  2. Balanced, Transparent, Risk-Informed Regimes
  3. Systemic Improvements
  4. Clear Rules on Compelled Provider Assistance
  5. Limitations on Lawful Hacking
  6. Limitations on Design Mandates
  7. Comprehensive Vulnerability Management
  8. Minimize Data Localization
  9. Periodic Review

Apple and Smartphone Encryption

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

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.

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

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

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

Apple and Google's operating systems run a combined **99.3% of smartphones** worldwide.

Source: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

As of January 18, 2018, 93 percent of all Apple devices are running iOS 10 or newer.

Source: https://developer.apple.com/support/app-store

Pre-iOS 8: Real Crimes, Real Victims

Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on smartphones and computers.

<u>Before Apple's September 2014 change</u>, crucial evidence was obtained from smartphones.

Homicide: People v. Hayes (Pre-iOS 8)

Indictment 04451/2012, New York State Supreme Court

An individual was recording a video on an iPhone when the defendant fatally shot him. The video was used at trial to corroborate eyewitness testimony. The shooter was convicted of murder at trial and sentenced to 35-years-to-life in state prison. If the phone had been encrypted and no one alive knew the passcode, the evidence would be lost.

Criminals are aware of the protection afforded by their encrypted devices.

A defendant in custody for a serious felony told a friend on a recorded jailhouse call that

> "Apple and Google came out with these softwares that can no longer be encrypted [SIC] by the police."
>
> He continued, "If our phones is running on the iO[S] 8 software, they can't open my phone. **That might be another gift from God."**

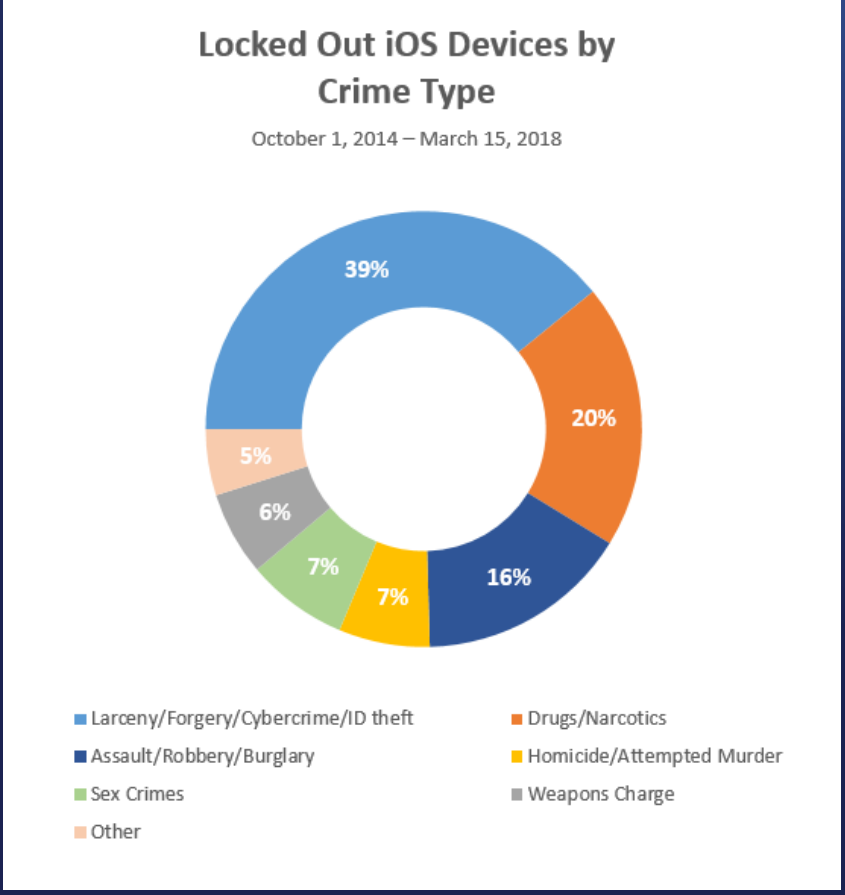
At the Manhattan DA's Office alone, **more than 1,675** iPhones lawfully-obtained since 2014 were inaccessible when they were seized.

Since 2014, **over 73%** of all Apple devices received by our digital forensics unit was locked.

These devices represent hundreds of real crimes against New Yorkers that cannot be fully investigated, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

Locked Status Upon Arrival 10/1/14-3/15/18						
	2014	2015	2016	2017	2018	Grand Total
ANDROID						
LOCKED	19	190	259	311	53	832
UNLOCKED	103	322	370	468	87	1350
ANDROID Total	**122**	**512**	**629**	**779**	**140**	**2182**
IOS						
LOCKED	58	382	536	564	135	1675
UNLOCKED	40	143	165	234	30	612
IOS Total	**98**	**525**	**701**	**798**	**165**	**2287**
GRAND TOTAL	**220**	**1037**	**1330**	**1577**	**305**	**4469**

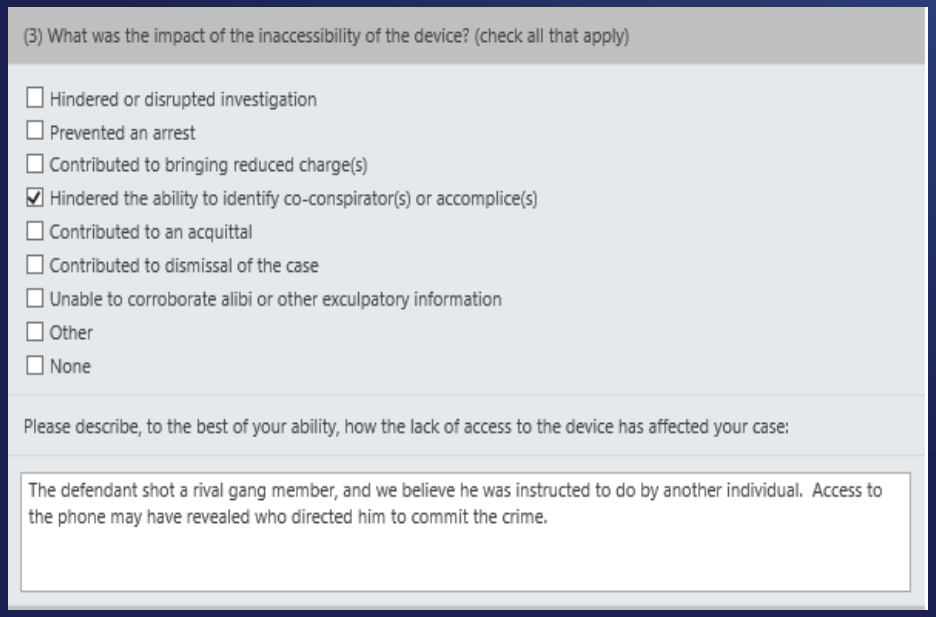
Received Locked Devices by Crime Type



- 7% Homicide/Attempted Murder
- 7% Sex Crimes
- 16% Assault/Robbery/Burglary

Measuring the Effect of Encryption on Cases

Question: What was the impact of inaccessibility of the device?



(3) What was the impact of the inaccessibility of the device? (check all that apply)

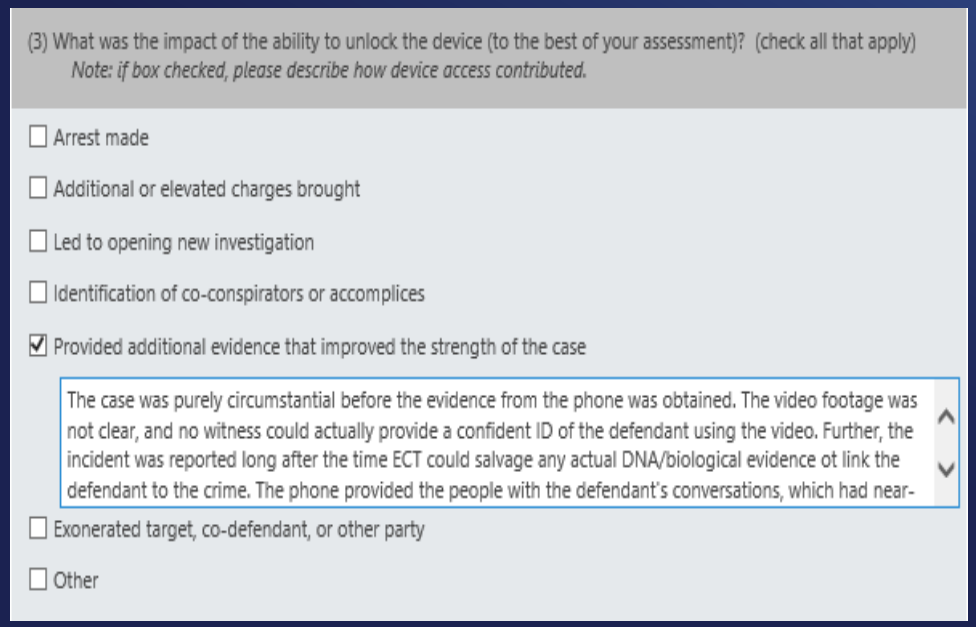
- ☐ Hindered or disrupted investigation
- ☐ Prevented an arrest
- ☐ Contributed to bringing reduced charge(s)
- ☑ Hindered the ability to identify co-conspirator(s) or accomplice(s)
- ☐ Contributed to an acquittal
- ☐ Contributed to dismissal of the case
- ☐ Unable to corroborate alibi or other exculpatory information
- ☐ Other
- ☐ None

Please describe, to the best of your ability, how the lack of access to the device has affected your case:

The defendant shot a rival gang member, and we believe he was instructed to do by another individual. Access to the phone may have revealed who directed him to commit the crime.

- 37.67% hindered or disrupted an ongoing investigation
- 24.16% hindered the ability to identify a co-conspirator

Value of Ability to Access Devices
Question: What was the impact of the ability to unlock the device?



(3) What was the impact of the ability to unlock the device (to the best of your assessment)? (check all that apply)
Note: if box checked, please describe how device access contributed.

- ☐ Arrest made
- ☐ Additional or elevated charges brought
- ☐ Led to opening new investigation
- ☐ Identification of co-conspirators or accomplices
- ☑ Provided additional evidence that improved the strength of the case

The case was purely circumstantial before the evidence from the phone was obtained. The video footage was not clear, and no witness could actually provide a confident ID of the defendant using the video. Further, the incident was reported long after the time ECT could salvage any actual DNA/biological evidence ot link the defendant to the crime. The phone provided the people with the defendant's conversations, which had near-

- ☐ Exonerated target, co-defendant, or other party
- ☐ Other

- 51.14% provided additional evidence
- 17 cases where evidence on a locked phone ultimately exonerated and/or mitigated the culpability of a target or co-defendant

Value of Ability to Access Devices

MURDER

- "This was a murder prosecution. Phone evidence provided (1) motive for crime, (2) partial admission to crime, (3) ability to conduct full investigation into potential cooperator before signing agreement."
- "Phone contained admissions by defendant that he possessed a firearm days before the shooting murder. Phone showed D efforts to hide following the crime. Phone connected D to the individuals captured on video with the murderer at the time of the crime."

Value of Ability to Access Devices

SEX CRIMES & CHILD PORNOGRAPHY

- "From the defendant's phone we obtained 3 videos which constituted CP and we brought a new indictment charging him with Promoting a Sexual Performance by a Child, Use of a Child in a Sexual Performance, Possessing a Sexual Performance by a Child, and Unlawful Surveillance.

  These videos were also strong corroboration of the CW's narrative in which she described the defendant entering her bedroom at night and raping her since the videos were all filmed during the night, in her bedroom, while she was sleeping and unaware."

FRAUD

- "We found audio recordings on the phones that supported our charges that the defendant was intentionally manipulating her victim through fraud and deceit."

Value of Ability to Access Devices: Exoneration / Mitigation

- “Phone corroborated owner's statement that he had not been present when shots were fired”

- “The information in this decedent's phone demonstrated that he died of a voluntary drug overdose.”

- “One video depicts defendant using PCP on night of murder, which is consistent with defense theory of NGRI”

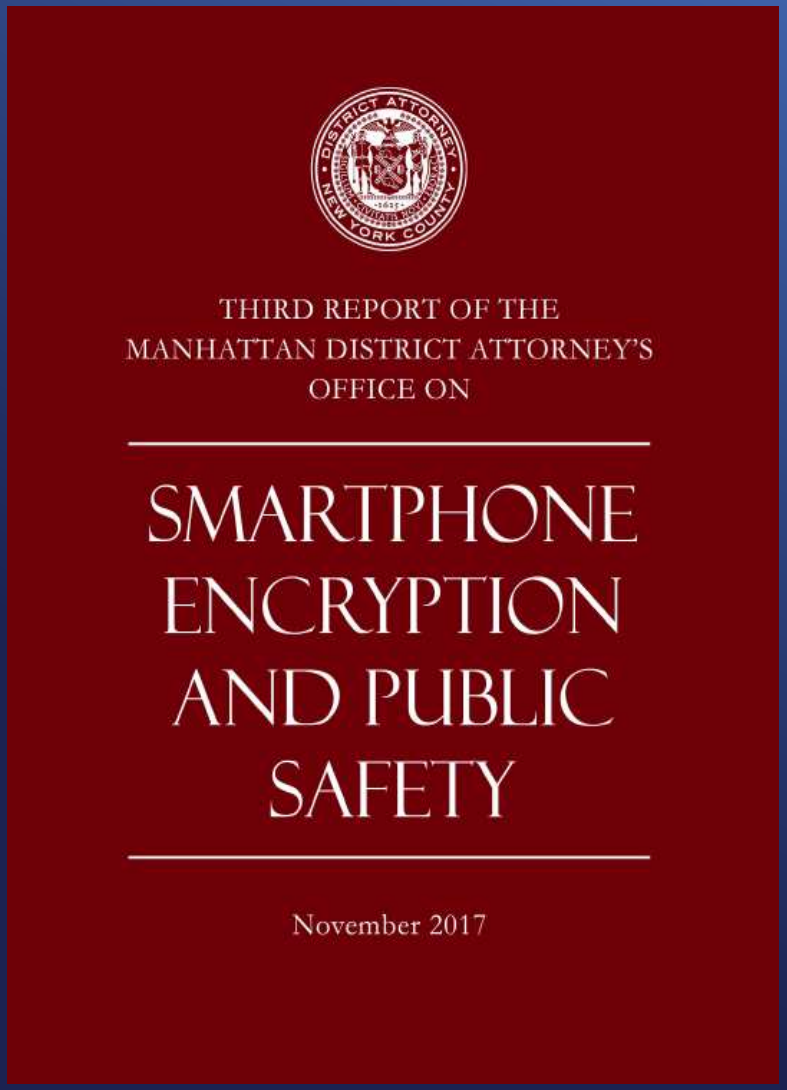
- “Corroborated defendant's statements that he was not present at the time of the crime in a one witness identification case”

Measuring the Effect of Encryption on Cases

- “Defendant and 2 others are alleged to have entered the victim's apartment and robbed him at gunpoint. Our inability to access the contents phone prevents us from seeing who he was in contact with before, during, or directly following the offense. While we can subpoena phone records, there is no other means to access text information or internet based communications such as FaceTime, WhatsApp, Facebook Messenger calls, etc.”

- “Defendant is seen using his phone immediately after the charged murder. Phone may have contained admissions going to defendant's state of mind and his justification defense.”

- “Case investigated by sex crimes as unlawful surveillance, it was reduced to a misdemeanor because we could not access the phone.”


THIRD REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON
SMARTPHONE
ENCRYPTION
AND PUBLIC
SAFETY
November 2017

Kenn Kern

Manhattan District Attorney's Office

Chief Information Officer

(212) 335-4021

KernK@dany.nyc.gov