



GENERAL COMMITTEE MEETING

**Thursday, June 18, 2020
3:00 PM to 4:00 PM**

Dial-In

888-432-1688; Room: 6597; User: 6328

1. **Welcome and Introductions**
2. **Guest speaker:**
John Riggi, American Hospital Association Attachment 1,2
Senior Advisor for Cybersecurity and Risk
3. **Legislative update** Attachment 3,4,5, 6
4. **Regulatory update** Attachment 7
5. **Monthly privacy round up** Attachment 8
6. **Articles of Interest** Attachment 9, 10, 11

Next Meeting: July 23, 2020 3:00-4:00pm



JOHN RIGGI

Senior Advisor for Cybersecurity and Risk

Experience Summary

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. John leverages his distinctive experience at the FBI and CIA in the investigation and disruption of cyber threats, international

organized crime and terrorist organizations to assist on policy and jriggi@aha.org advocacy issues and provide trusted advisory services for the nations'

(O) +1 202-626-2272 hospitals and health systems. His trusted access to hospital leadership (M) +1 202-640-9159 and government agencies enhances John's national perspective and ability to provide uniquely informed risk advisory services.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He was also the FBI national operations manager for terrorist financing investigations. John led the FBI Cyber Division national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the investigation of the largest cyber attacks targeting healthcare and other sectors.

John currently co-leads a national HHS/healthcare sector task group to develop resources to assist the field in managing cyber risk as an enterprise risk issue. John launched a national campaign with the AHA and government agencies to help members protect medical research against foreign threats.

He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest award in this category. John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media.



The COVID Cyber and Privacy Threat Landscape

A blue banner with a background of interlocking gears and a white padlock icon in the center. The American Hospital Association logo and tagline are positioned in the upper right of the banner.

American Hospital Association™
Advancing Health in America

Cybersecurity and Risk Advisory Services



Presented by John Riggi, Senior Advisor, Cybersecurity and Risk Advisory Services 6/18/2020



Agenda

- COVID-19 Cyber Threats Update
- Cyber Attack Methodology
- Cyber and Privacy Policy Issues + Resources



Corona Virus and Cyber Viruses: Cyber Criminals Exploiting a Crisis

Ventilators and Life Support Devices

Phishing Emails

Telehealth and Telework
vulnerabilities

Cloud Vulnerabilities

Malicious Sites

Online Fraudulent PPE Schemes

Supply Chain Risk

Theft of research on treatments and vaccine



Coronavirus Themed E-mail Phishing
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV

**NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY**

Fake Online Coronavirus Map Delivers Well-known Malware
Health Sector Cybersecurity Coordination Center (HC3)
TLP:GREEN

**OFFICE of
PRIVATE SECTOR**

**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL — OFFICE OF INVESTIGATIONS
DIGITAL INVESTIGATIONS BRANCH**

FBI FLASH
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21MAY2020
Alert Number
AC-000128-LD

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email:
cywatch@fbi.gov
Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and*

Graphic 1: Example Numbers

As a result of unconfirmed OI/DIB has identified a Critical Infrastructure P Department and HPH d

Graphic 2: Example Numbers

In preparation for Covid major online retail source the IT staff noted that n this type activity could Providers purchasing re assume the condition o

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats.

This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Nation State Cyber Actors Target US Organizations Conducting COVID-19 Research

Summary

Nation-state cyber actors are targeting many domestic universities, research institutes, and private companies conducting COVID-19-related research. The FBI has observed malicious cyber actors conducting vulnerability scanning, reconnaissance activity, and attempted data exfiltration from entities involved in COVID-19 research and associated clinical trials. The potential compromise and theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options and the United States' efforts to respond to the ongoing crisis.

Update: After cybersecurity threat, Arkansas Children's Hospital systems getting back online



COVID-19 Complication: Ransomware Keeps Hitting Healthcare

Cybercrime Continues Despite Pandemic Intensifying

Mathew J. Schwartz (@euroinfosec) · March 16, 2020

Posted: Mar 10, 2020 / 1

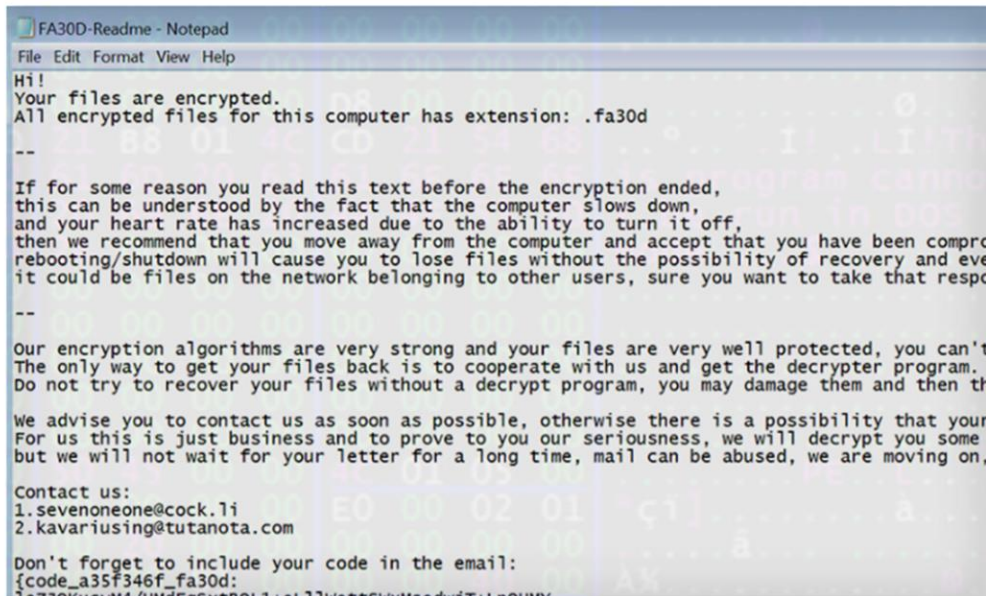
Share buttons for Twitter, Facebook, LinkedIn, and a 'Get Permission' button.

Update:

LITTLE ROCK, Ark. - last week.

ACH issued this up

"We are bringing our online and available. refining our online connectivity.



Ransom note for Netwalker ransomware, tied to a recent attack against Champaign-Urbana Public Health District in Illinois (Source: Carbon Black)

Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak

The hospital has one of the largest COVID-19 testing facilities in the Czech Republic.

By Sophie Porter | March 19, 2020 | 06:58 AM



Czech Republic was hit by a massive computer shutdown in the

the largest COVID-19 testing facilities for operations and relocate new pa

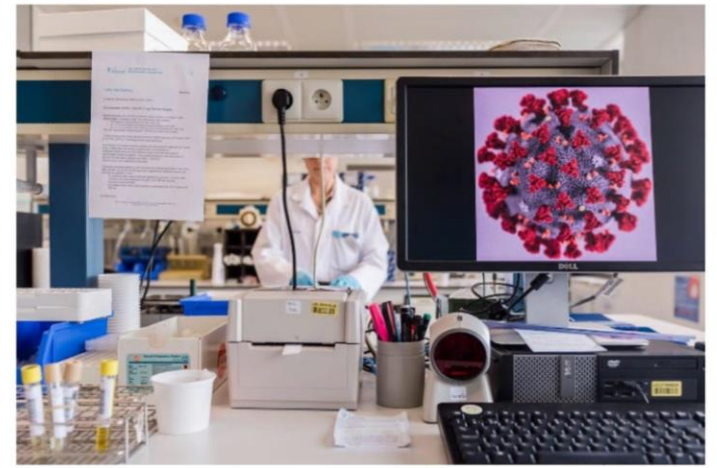
Colorado Hospital Patient Information System Hit by Crypto Ransomware

Hackers have infected the infrastructure of Parkview Medical Center with ransomware that demands cryptocurrency in exchange for an encryption key.

6600 Total views 94 Total shares Listen to article 2:16



This is not the time to leave our hospitals unprotected against cyberattacks



A magnified coronavirus germ is displayed on a computer in the virology research labs at UZ Leuven university hospital in Belgium on Feb. 26. (Geert Vanden Weyngaert/Bloomberg)

By Allison Peters and Ishan Mehta March 19 at 1:27 PM

“A ransomware attack on a hospital is a not just an economic crime, it’s a threat to life crime...and it should be prioritized, pursued and prosecuted as such ”

John Riggi, AHA Senior for Cybersecurity and Risk





TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 May 2020

Alert Number
MI-000124-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH** immediately.

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

COVID-19 Phishing Email Indicators

Summary

The FBI uncovered targeted email phishing attempts to harvest user credentials and compromise targets' computer systems by exploiting fear derived from the COVID-19 pandemic. Through investigations, the FBI continues to identify multiple COVID-19 email phishing campaigns with malicious file attachments and URLs. The following associated indicators of compromise (IOCs) are being provided to assist in network defense.

Technical Details

Cybercriminal and advanced persistent threat (APT) groups are leveraging COVID-19 themed health, informational, and warning notice emails in an attempt to obtain online service credentials, e.g., Microsoft O365 accounts. These emails direct targets to click links by purporting to be online services requiring authentication. Malicious actors use these links to capture victim credentials and then redirect victims to the World Health Organization's (WHO) Coronavirus notice. Additionally, cybercriminals and APT groups have attached archive files that contain malicious portable executables (PE) or JAVA.jar files to their phishing emails, outlined in the table below.



TLP:GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 MAY 2020

Alert Number
MI-000125-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH** immediately.

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Indicators of Compromise Associated with ProLock Ransomware

Summary

As of March 2020, the FBI received notification that the ransomware variant ProLock had infected multiple organizations in the United States to include healthcare organizations, government entities, financial institutions, and retail organizations. ProLock was previously released as PwndLock ransomware in early March 2020. ProLock actors instruct victims to pay the ransom in several days, threatening to release the victims' data on social media and public websites.

Technical Details

ProLock actors gain initial access to victim networks through phishing emails, Qakbot,¹ improperly configured remote desktop protocol (RDP), and stolen login credentials for networks with single-factor authentication. After ProLock actors gain access to a victim's network, they map the network and identify backups, to include Volume Shadow Copies, for deletion and/or encryption.

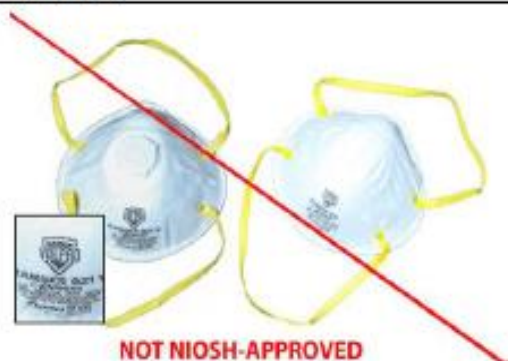


OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



Graphic 1: Example of Fraudulent N95 Respirator TC 84A-007 Using 3M's NIOSH Approval Numbers



This is an example of two respirators with fraudulent NIOSH markings. Valpro Safety is selling the Ranger 821 and Ranger 821V respirators using the 3M approval number (TC-84A-007) and label without 3M's permission. (Source: <https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html>)

Graphic 2: Example of Fraudulent N95 Respirator TC 84A-0427 Using 3M's NIOSH Approval Numbers



This is an example of a respirator with fraudulent NIOSH markings. The NT-V2 Nano Bi-Directional respirator is being advertised as if it is NIOSH-approved, including a NIOSH approval number. While the TC number (TC 84A-0427) is valid, it does not belong to Pasture Pharma. Instead, TC 84A-0427, is an approval number for a 3M full facepiece respirator with cartridges. (Source: <https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html>)

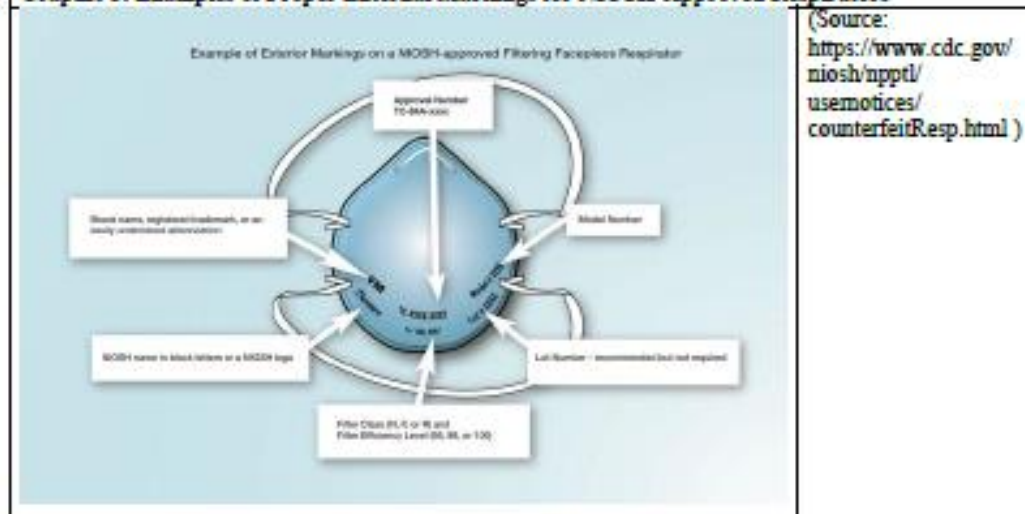


OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



Graphic 3: Examples of Proper External Markings for NIOSH-Approved Respirators



3M distribution centers inside the United States do import N95 models 1870+, 9210+, and 9211+ directly from 3M's manufacturing facilities overseas. This occurs, however, within 3M's own internal supply chain operations.

- Importation of 3M respirator products, particularly in high volumes, to non-3M distribution centers or unauthorized resellers² should be considered suspicious.

Indicators of Fraudulent or Counterfeit Sales of 3M Personal Protective Equipment

Fraudsters may either purport to be 3M as part of a scam, or may claim to be a distributor. Some of the most common tactics used by criminals include the following:

- Most fraudsters demand up-front payment, when 3M does not request advance payment.
- Fraudsters may claim access to significant inventories of 3M PPE. They often claim to be able to export products from a country where 3M products are not sold or distributed.

Graphic 4: Single-Respirator List Prices for the Most Common 3M N95 Respirator Models Sold in the US

	Model #	List Price (USD)
Surgical N95 Respirators	1804	\$0.68
	1804S	\$0.68
	1860	\$1.27
	1860S	\$1.27
	1870+	\$1.78
Standard N95 Respirators	8210	\$1.02 - \$1.31
	8210Plus	\$1.18 - \$1.50
	8210V	\$1.48 - \$1.88
	8110S	\$1.08 - \$1.37
	8200	\$0.63 - \$0.80
	8511	\$2.45 - \$3.11
	9105	\$0.64 - \$0.81
	9105S	\$0.64 - \$0.81
	9210+	\$1.40 - \$1.78
	9211+	\$2.68 - \$3.40

(Source: <https://multimedia.3m.com/mws/media/18036700/fraudulent-activity-price-gouging-and-counterfeit-products.pdf>)



ACTIVITY ALERT

Joint Activity Alert

AA20-133A

NUMBER

May 12, 2020

DATE

Top 10 Routinely Exploited Vulnerabilities

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

This alert provides details on vulnerabilities routinely exploited by foreign cyber actors—primarily Common Vulnerabilities and Exposures (CVEs)¹—to help organizations reduce the risk of these foreign threats.

Foreign cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations. Exploitation of these vulnerabilities often requires fewer resources as compared with zero-day exploits for which no patches are available.

The public and private sectors could degrade some foreign cyber threats to U.S. interests through an increased effort to patch their systems and implement programs to keep system patching up to date. A concerted campaign to patch these vulnerabilities would introduce friction into foreign adversaries' operational tradecraft and force them to develop or acquire exploits that are more costly and less widely effective. A concerted patching campaign would also bolster network security by focusing scarce defensive resources on the observed activities of foreign adversaries.

For Malware Initial Finding Reports and Malware Analysis reports associated with the CVEs in this alert, see <https://www.us-cert.gov/ncas/alerts/aa20-133a>.

<https://www.us-cert.gov/ncas/alerts/aa20-133a>

¹ <https://cve.mitre.org/cve/>

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp/>.



TLP:WHITE



TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21MAY2020

Alert Number

AC-000128 -LD

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and respond to threats.*

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats.

This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Nation State Cyber Actors Target US Organizations Conducting COVID-19 Research

Summary

Nation-state cyber actors are targeting many domestic universities, research institutes, and private companies conducting COVID-19-related research. The FBI has observed malicious cyber actors conducting vulnerability scanning, reconnaissance activity, and attempted data exfiltration from entities involved in COVID-19 research and associated clinical trials. The potential compromise and theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options and the United States' efforts to respond to the ongoing crisis.

TLP: WHITE



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 MAY 2020

PIN Number

20200521-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:

www.fbi.gov/contact-us/field

E-mail:

cywatch@fbi.gov

Phone:

1-855-292-3937

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats.

This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This PIN has been released **TLP: WHITE**: Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Criminals and Nation-State Cyber Actors Conducting Widespread Pursuit of US Biological and COVID-19 Related Research

Summary

Criminal and nation-state cyber actors since February 2020 have been increasingly targeting US pharmaceutical, medical, and biological research facilities to acquire or manipulate sensitive information, to include COVID-19 vaccine and treatment research amid the evolving global pandemic. The US Healthcare and Public Health Sector (HPH), including pharmaceutical and medical companies, has been a common target of malicious cyber activity even prior to the pandemic. This notification seeks to raise awareness in the HPH sector by highlighting the current threat and cyber tactics used by our adversaries.

FOR IMMEDIATE RELEASE

Thursday, June 11, 2020

Officer of China's People's Liberation Army Arrested At Los Angeles International Airport

Defendant Charged with Visa Fraud, Arrested At Airport While Planning To Leave the United States

SAN FRANCISCO – Xin Wang, a scientific researcher and officer with the People's Republic of China's (PRC) People's Liberation Army (PLA), was arrested at Los Angeles International Airport (LAX) while attempting to depart the United States for Tianjin, China, and was charged with visa fraud, announced United States Attorney David L. Anderson and Federal Bureau of Investigation Special Agent in Charge John F. Bennett.

According to court documents filed today and a complaint which was unsealed on Monday, Wang entered the United States on March 26, 2019, after receiving a multiple entry J1 non-immigrant visa in December of 2018. Wang's visa application stated that the purpose of his visit was to conduct scientific research at the University of California, San Francisco (UCSF). Wang is alleged to have made fraudulent statements on this visa application. Specifically, in his visa application, Wang stated that he had served as an Associate Professor in Medicine in the PLA, from September 1, 2002 through September 1, 2016.





TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020

PIN Number
20200521-003

Please contact the FBI with any questions related to this Private Industry Notification at either your local Cyber Task Force or FBI CyWatch.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Cyber Criminals Take Advantage of COVID-19 Pandemic to Target Teleworking Employees through Fake Termination Phishing Emails and Meeting Invites

Summary

In response to the recent increase in teleworking during the COVID-19 pandemic, cyber criminals are targeting teleworking employees with fraudulent termination phishing emails and VTC meeting invites, citing COVID-19 as the reason. Employees who are alarmed by the message may not scrutinize the spoofed email address that looks similar to their company's legitimate one. The emails entice victims to click on malicious links purporting to provide more information or online conferences pertaining to the victim's termination or severance packages. Companies should alert their employees to look for emails coming from Human Resources or management with spoofed email domains.



TLP:GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020

PIN Number
20200521-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local Cyber Task Force or FBI CyWatch.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
CyWatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:GREEN**: The information in this product is useful for the awareness of all participating organization with their sector or community, but should not be shared via publicly accessible channels.

Computer-Assisted Dispatch Systems Vulnerable to Ransomware Attacks Against Local and Tribal Government

Summary

Cyber actors continue to target local and tribal government computer systems to deny essential services and force ransom payments. Recent attacks have disabled computer-assisted dispatch (CAD) systems operated by county sheriff departments, hindering response capability.

CAD software is used by government—specifically, public safety and 911/311 call centers—to more efficiently manage resources through integration with geographic information systems (GIS), traffic flow data, and other information to execute service requests. Emergency call centers use CAD to identify the location of calls for emergency assistance, display call history for specific addresses, connect to law enforcement databases, and identify potential hazards. CAD systems' connectivity to other public safety IT networks could allow



TLP:AMBER

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

5 MAY 2020

Alert Number
MU-000126-MW

**WE NEED YOUR
HELP!**

If you find any of these indicators on your networks, or have related information, please contact

**FBI CYWATCH
immediately.**

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

Latest Tactics, Techniques, and Procedures Associated with Ryuk Ransomware and Recommended Mitigation

Summary

Unknown cybercriminals have targeted more than 1,000 US and international businesses with Ryuk ransomware since approximately August 2018. Once the victim has been compromised, Ryuk encrypts all the network's data files and the actors demand sums of up to \$24 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk impacts a range of industries, attacks have had a disproportionate impact on logistics companies, technology companies, healthcare organizations, and municipalities.

Technical Details

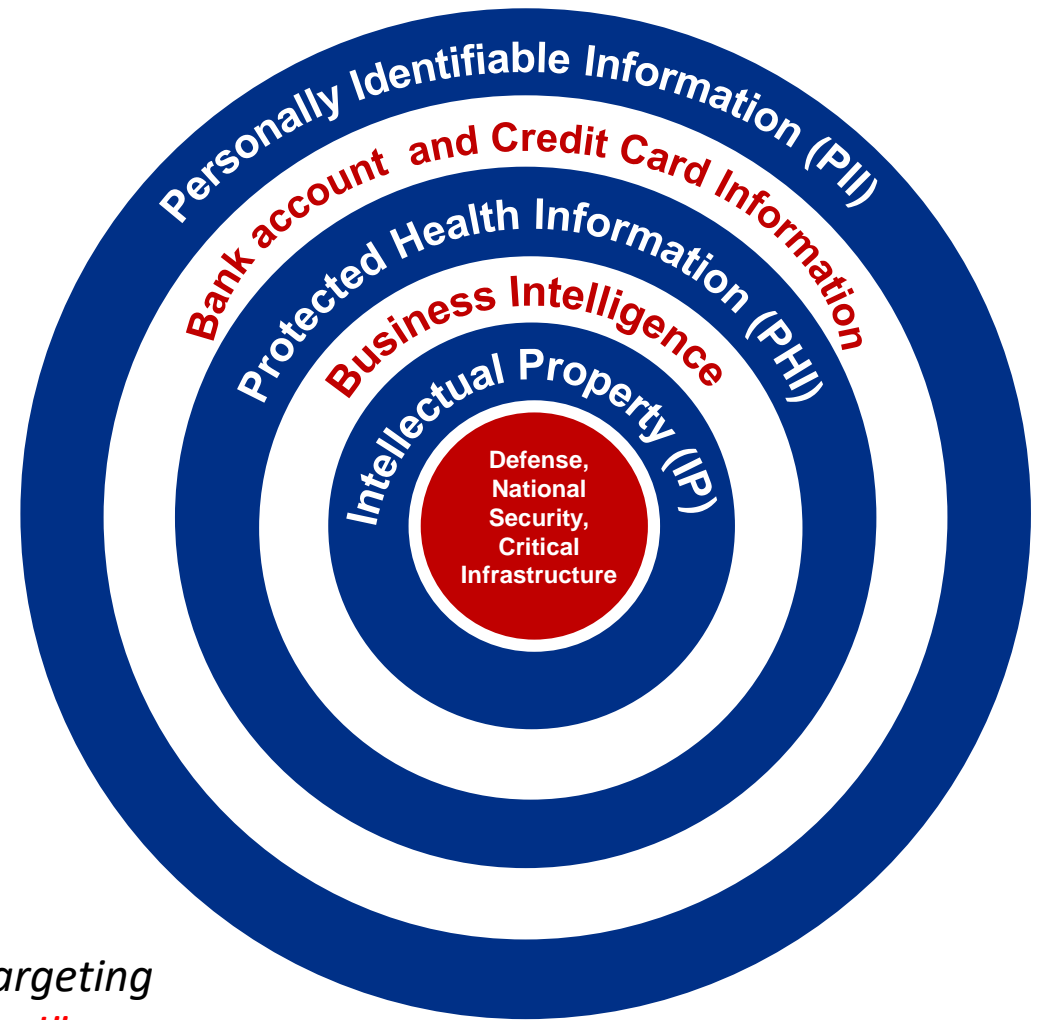
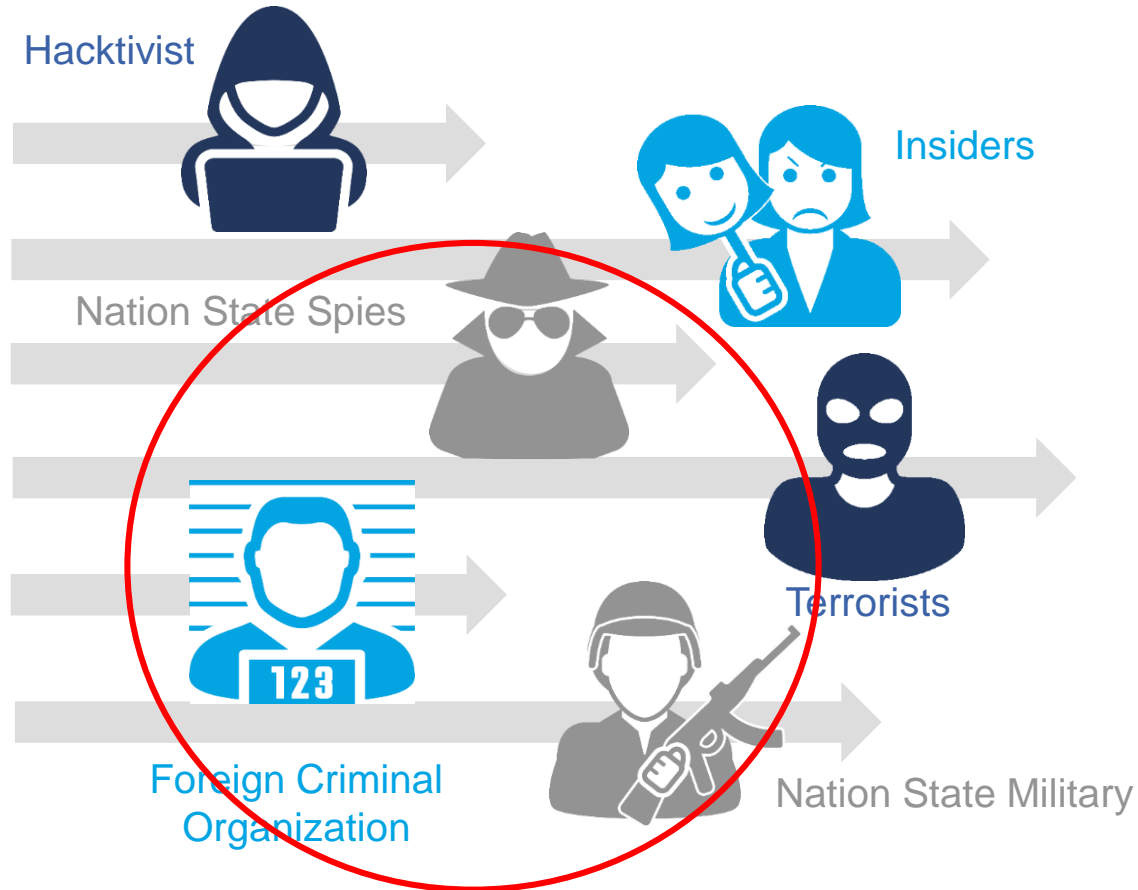
Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the "HERMES" tag but in some infections the files have

TLP:AMBER

Comments and Questions?

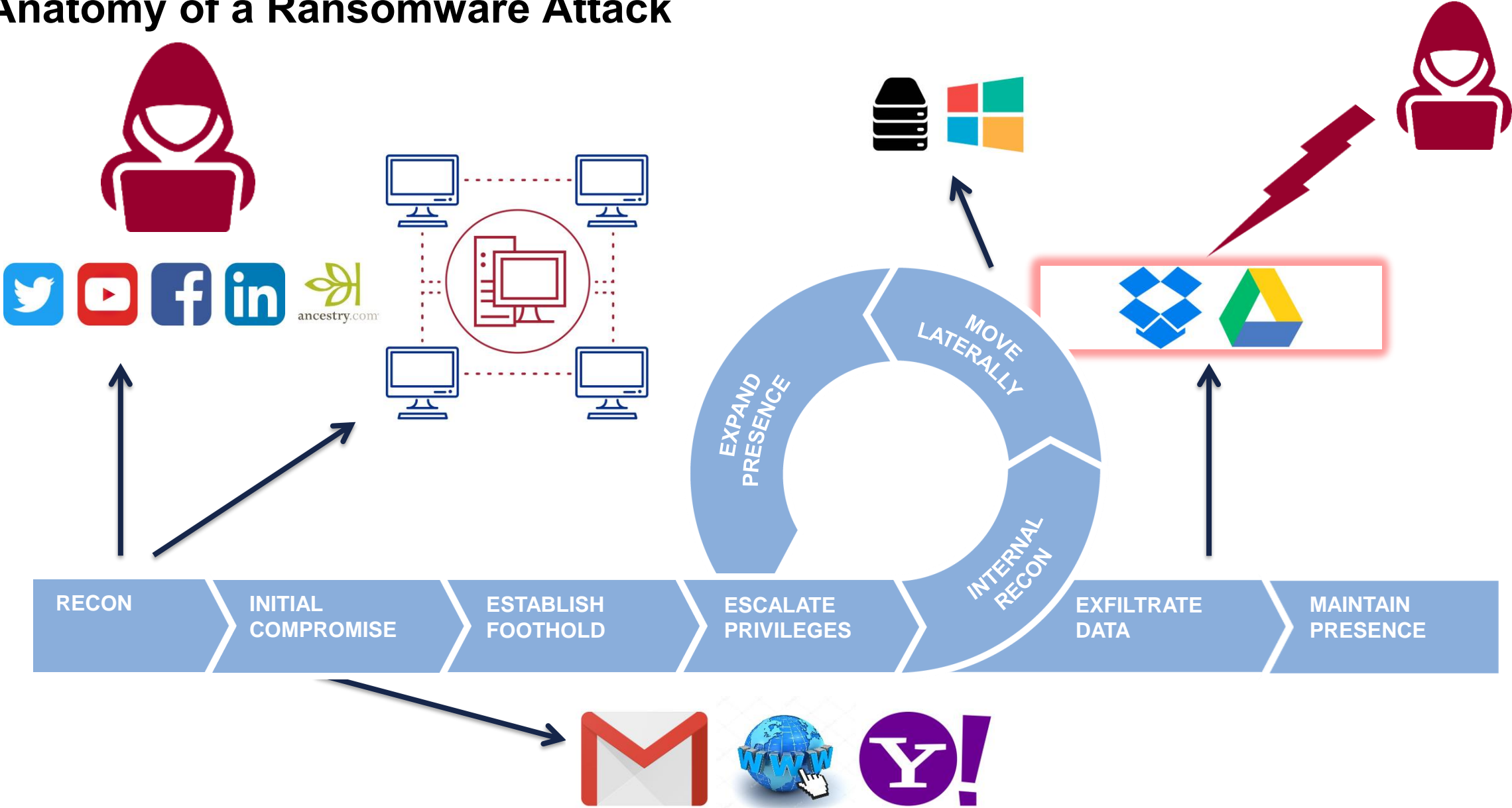
Data Rich Environment = Target Rich Environment

Targeted Data



*Nation states, criminals, insiders and hackers are aggressively targeting healthcare providers to steal their valuable data. **“One stop hacking!”***

Anatomy of a Ransomware Attack



Types of Social Media



- There are many categories of social media, the most common:
Social Networking

- Examples:

- Facebook
- Myspace (obsolete)
- Google (obsolete)
- LinkedIn
- Twitter

- Many other categories:

- Pictures/Images
 - Snap Chat
 - Instagram
 - Flickr
- Knowledge/Discussion
 - Wikipedia
 - Academia
 - Reddit
- Music
 - Pandora
 - Spotify
 - Rhapsody




Image source: Conversation Prism 5.0


Impact of Social Media Breaches



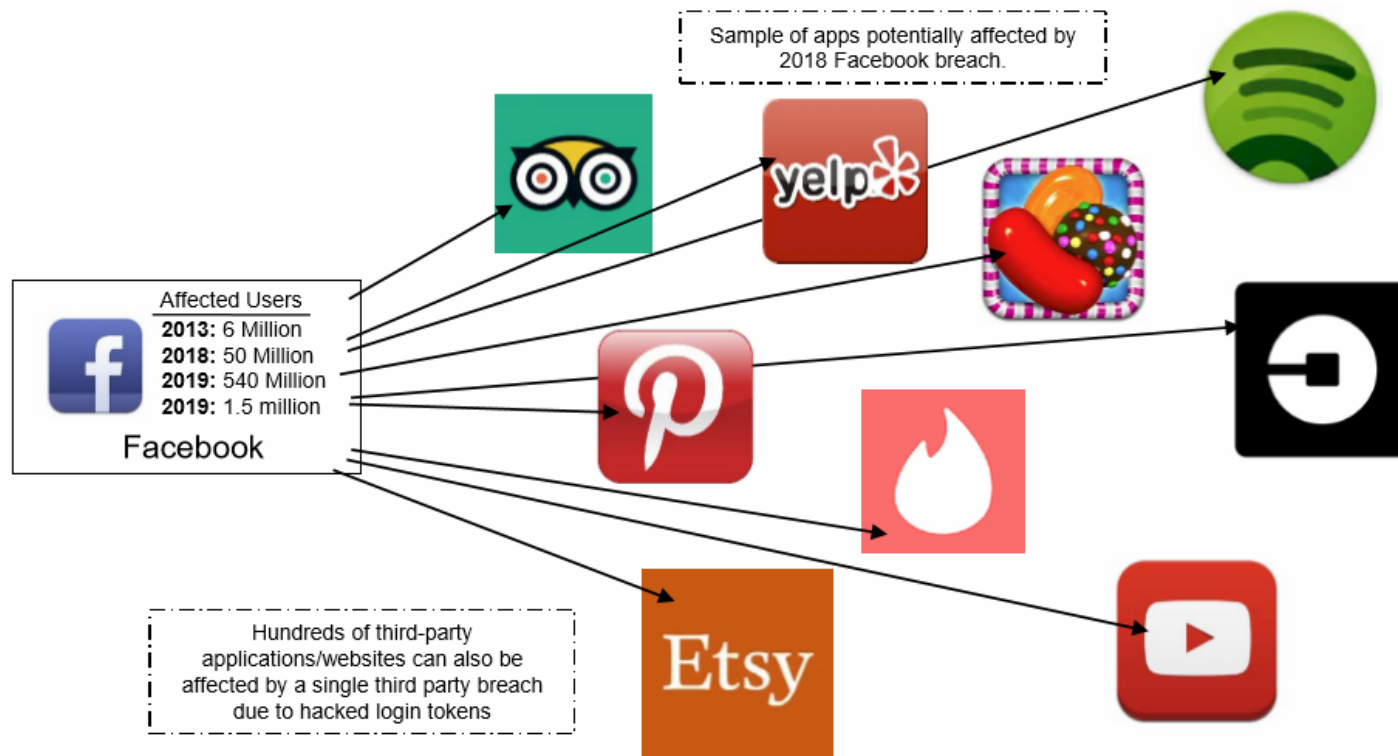
- While breaches of social media websites/companies only make up less than one percent of all data breaches per year, the incidents account for over 56% of ALL compromised data.

 **Affected Users**
2018: 52.5 Million
Google+

 **Affected Users**
2013: 250,000
2016: 32.8 Million
2018: 330 Million
Twitter

 **Affected Users**
2013: 4.6 Million
2017: 55,000
Snapchat

 **Affected Users**
2012: 6.5 Million
2016: 167 Million
LinkedIn



The extent to how much specific data is compromised across the internet due to a single social media breach still can not be ascertained due to the sheer amount of apps that can be accessed with third party login credentials.

Comments and Questions?



Detection and Risk Controls: EG - 3C

- **EDUCATE** - Create awareness and support among leadership, researchers and staff *in an audience sensitive manner*, of the foreign influence threats to medical research and innovation. Discuss real world implications.
- **GOVERNANCE** - Identify a function and senior accountable executive who will have overall responsibility and sufficient independence, authority and status to coordinate and lead the process across multiple functions.
- **CATALOGUE** - All research and intellectual property
 - Where are the *multiple* locations it is stored, *who has access, internally and remotely* ?
- Risk **CLASSIFY and STRATIFY** research data in terms of impact to:
 - Public Health and Safety
 - Dual Use – Military Application, weaponization
 - National Security
 - Economic Security
 - Business Risk – What is the value? Strategic implications, economic value, loss of innovation, reputation
- Outside expertise and government assistance (FBI, DHS, HHS, NIH and Commerce) - **Ongoing Process**
- **CONTROL** – Based upon risk classification and stratification. Combination of personnel, legal, physical and information security controls.



Risk Prioritization and Impact

Do we prioritize all strategic threats, cybersecurity policies, procedures, controls and technical risks by **impact** to:

REPUTATION

1. **Care delivery and PATIENT SAFETY - first and always**
2. Mission critical operations
3. Confidence of patients, staff, community and investors
4. Protection and privacy of data - including health records, personally identifiable information, financial and payment data and intellectual property*
5. Revenue
6. Legal and regulatory exposure
7. Mergers and acquisitions



HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency

We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.

Non-public facing technologies, such as FaceTime or Skype allowed.

Good faith provision of telehealth during the COVID-19 nationwide public health emergency

Public facing apps such as Facebook Live, Twitch, TikTok, and similar are prohibited

Notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes





March 2020

COVID-19 & HIPAA Bulletin
Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

The Novel Coronavirus Disease (COVID-19) outbreak imposes additional challenges on health care providers. Often questions arise about the ability of entities covered by the HIPAA regulations to share information, including with friends and family, public health officials, and emergency personnel. As summarized in more detail below, the HIPAA Privacy Rule allows patient information to be shared to assist in nationwide public health emergencies, and to assist patients in receiving the care they need. In addition, while the HIPAA Privacy Rule is not suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

In response to President Donald J. Trump's declaration of a nationwide emergency concerning COVID-19, and Secretary of the U.S. Department of Health and Human Services (HHS) Alex M. Azar's earlier declaration of a public health emergency on January 31, 2020, Secretary Azar has exercised the authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient's right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient's right to request confidential communications. See 45 CFR 164.522(b).

CMS adds 85 more Medicare services covered under telehealth

Jackie Drees - 6 hours ago [Print](#) | [Email](#)



CMS on March 30 [issued](#) various regulatory [changes](#) to further support hospitals', physicians' and other healthcare organizations' capabilities during the COVID-19 pandemic, including expanding Medicare coverage of telehealth visits.

On March 17, the Trump administration [announced](#) CMS will temporarily pay clinicians to provide telehealth services for beneficiaries during the pandemic. CMS is now expanding Medicare coverage of 85 additional services provided via telehealth, including emergency department visits and initial nursing facility and discharge visits.

Here are the 85 additional services, and their respective codes, that CMS will cover when provided via telehealth through the duration of the pandemic:

[Global Edition](#) [Privacy & Security](#)

AMA, AHA partner on COVID-19 cyber threats guidance for hospitals, physicians

As opportunistic attacks ramp up, the groups offer recommendations for VPNs and cloud-based services, coronavirus-themed phishing emails, telehealth

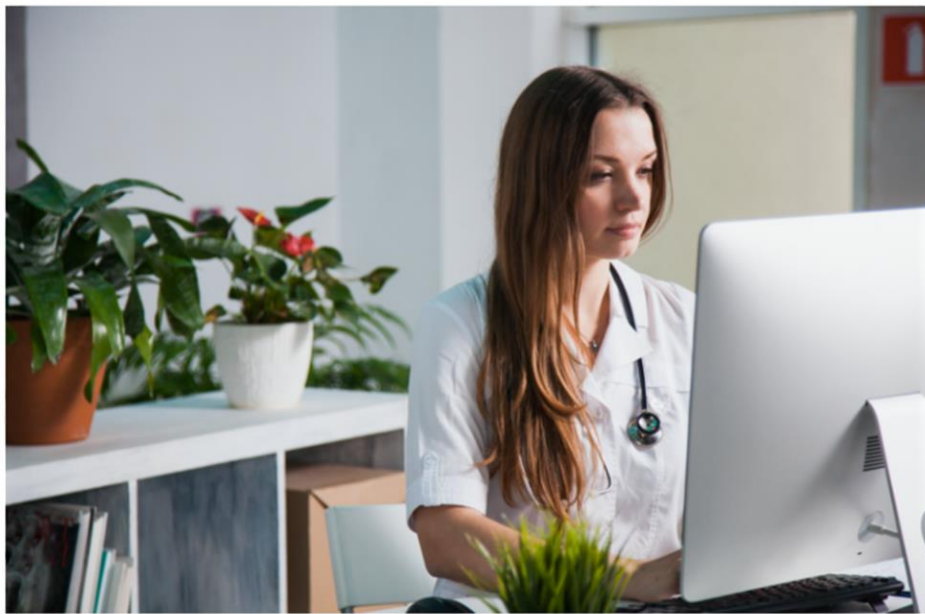
FierceHealthcare

HOSPITALS & HEALTH SYSTEMS TECH PAYER FINANCE PRACTICES REGULATORY COVID-19 S

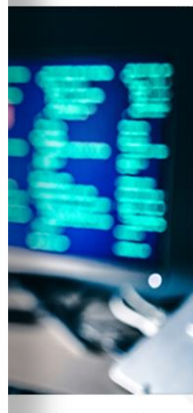
Practices

AMA and AHA team up to launch resource to fight malicious cyberactivity

by Tina Reed | Apr 15, 2020 3:05pm



The American Medical Association and the American Hospital Association teamed up to launch new guidance to fight malicious cyber activity in the midst of the COVID-19 pandemic. (klyots/shutterstock)



WHAT PHYSICIANS NEED TO KNOW

Working from home during COVID-19 pandemic

During the COVID-19 pandemic, many physicians are working from home, using their personal computers and mobile devices to help care for patients. Fortunately, technology can allow physicians and care teams to do much of what they could do at the medical office, remotely. Telemedicine is a powerful tool that spans a continuum of technologies and offers new ways to deliver care. Many electronic health record (EHR) systems allow you to connect over the Internet just as if you were in the clinic. While you are doing your part to help during the COVID-19 pandemic, the American Medical Association (AMA) and American Hospital Association (AHA) want to ensure you have resources to help keep your work environment safe from cyber-threats that could disrupt your practice, the hospital, or negatively impact your patients' safety and well-being.

Your Home Personal Computer (PC)

Your home computer, whether it be a Windows or Mac, laptop or desktop, is susceptible to cyber threats. It is important to take steps to keep your home office as resilient as your medical practice. We are learning of increased security threats to medical data due to the pandemic. Many cyber criminals are taking advantage of clinician interest in COVID-19 to infect practices, and hospitals' computers and networks with the hope of stealing or holding medical records for ransom.

To help protect you and your patients, the AMA has compiled a [Checklist for Computers](#), which is a non-exhaustive list of **actions you should take immediately** to strengthen your home computer and network.

• Watch out for these common threats:

- **E-mail phishing** is an attempt to trick you into giving out information using e-mail. E-mail cybersecurity should remain a top priority for clinicians and hospitals as a vast majority of cyber-attacks are initiated by clicking on a phishing e-mail containing malware (malicious software) or a malicious link appearing to be COVID-19 related from a legitimate organization. Additional information on e-mail phishing can be [found at this resource](#) on pages 16-17. The FBI has also issued several Public Service Announcements on business email frauds and COVID-19 themed frauds and they can be found [here](#).
- **Ransomware** is a type of malware (malicious software) that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker who deployed the malware until a ransom is paid. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. The FBI discourages paying the ransom as it may incentivize continued ransomware attacks and fund more serious crimes including violent crimes. Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Additional information on ransomware can be [found at this resource](#) on pages 18-19.

CMS Interoperability and Patient Access final rule

Overview:

The Interoperability and Patient Access final rule (CMS-9115-F) delivers on the Administration's promise to put patients first, giving them access to their health information when they need it most and in a way they can best use it. As part of the Trump Administration's MyHealthEData initiative, this final rule is focused on driving interoperability and patient access to health information by liberating patient data using CMS authority to regulate Medicare Advantage (MA), Medicaid, CHIP, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FHEs).

This rule finalizes new policies that give patients access to their health information and moves the healthcare system toward great interoperability. These new policies include:

- Patient Access API (*applicable January 1, 2021*)
- Provider Directory API (*applicable January 1, 2021*)
- Payer-to-Payer Data Exchange (*applicable January 1, 2022*)
- Improving the Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges (*applicable April 1, 2022*)
- Public Reporting and Information Blocking (*applicable late 2020*)
- Digital Contact Information (*applicable late 2020*)
- Admission, Discharge, and Transfer Event Notifications (*applicable fall 2020*)

Read the [Fact Sheet](#) to learn more about these new policies.

To view the CMS Interoperability and Patient Access final rule, [download the PDF \(PDF\)](#).

To view the ONC 21st Century Cures Act final rule, visit <https://www.healthit.gov/curesrule>.

ONC officials describe requirements of new API, information blocking rules

National Coordinator Don Rucker and Deputy National Coordinator Steve Posnack talk enforcement timelines, "content and manner," FHIR 4, gag clause provisions, patient privacy and more.

By [Mike Mitiard](#) | March 09, 2020 | 03:16 PM



ONC's Dr. Donald Rucker and Steve Posnack.

The long-awaited interoperability and information blocking final rules published by the Office of the National Coordinator for Health IT on Monday will require some big changes to the ways healthcare organizations – specifically providers, certified health IT developers and health information networks and exchanges – have been used to doing things.

The sweeping new regs – which update software certification requirements, mandate APIs usable "without special effort" and put rules in place to combat information blocking and anti-competitive practices – will require some significant cultural adjustments and material investments from healthcare orgs hoping to stay compliant with the law.

Health Industry Publishes Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)



Health Industry Publishes Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)

Washington, D.C., May 18, 2020 - The Health Sector Coordinating Council (HSCC) and the Health Information Sharing and Analysis Center (H-ISAC), today jointly released a tactical guide for how healthcare organizations can manage cybersecurity threats that occur during a crisis such as the COVID-19 pandemic.

The [Health Industry Cybersecurity Tactical Crisis Response \(HIC-TCR\) Guide](#) is constructed to advise health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency. Smaller organizations can leverage this document as a list of activities to consider. Larger organizations can use it as a sanity check for existing plans.

The HIC-TCR also implements a major recommendation in a 2017 report by the [Health Care Industry Cybersecurity \(HCIC\) Task Force](#), that “Industry should implement cybersecurity incident response plans, which are reviewed and tested annually.” The HCIC Task Force was appointed and co-led by the U.S. Department of Health and Human Services and industry executives pursuant to the Cybersecurity Act of 2015, and has been a guiding reference for the HSCC to address cybersecurity challenges facing the health sector.

“During a crisis, technology, processes and even the way we work can change on a dime; this opens up brand new attack surfaces, and the vulnerability from malicious cyber-attacks increases as well,” said Erik Decker, Chief Information Security and Privacy Officer of University of Chicago Medicine and a co-lead of the task group that produced the report. “To thwart these attacks before they occur, it is essential for health care organizations to analyze, establish, implement, and maintain cybersecurity practices that are responsive to the crisis at hand.”

<https://healthsectorcouncil.org/health-industry-publishes-health-industry-cybersecurity-tactical-crisis-response-guide-hic-tcr/>



jriggi@aha.org

(O) +1 202-626-2272

(M) +1 202-640-9159

JOHN RIGGI

Senior Advisor for Cybersecurity and Risk

Experience Summary

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. In this role, John leverages his distinctive experience at the FBI and CIA in the investigation and disruption of cyber threats, international organized crime and terrorist organizations to provide trusted advisory services for the leadership of hospitals and health systems across the nation. His trusted access to hospital leadership enhances John's national perspective and ability to provide uniquely informed risk advisory services.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He also led the FBI Cyber national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors to assist these sectors defend against cyber attacks. John held a national strategic role in the investigation of the largest cyber breaches impacting healthcare and other critical infrastructure sectors. He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest award in this category.

Questions?

LINDSEY O. GRAHAM, SOUTH CAROLINA, CHAIRMAN

CHARLES E. GRASSLEY, IOWA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
BEN SASSE, NEBRASKA
JOSHUA D. HAWLEY, MISSOURI
THOM TILLIS, NORTH CAROLINA
JONI ERNST, IOWA
MIKE CRAPO, IDAHO
JOHN KENNEDY, LOUISIANA
MARSHA BLACKBURN, TENNESSEE

DIANNE FEINSTEIN, CALIFORNIA
PATRICK J. LEAHY, VERMONT
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT
MAZIE HIRONO, HAWAII
CORY A. BOOKER, NEW JERSEY
KAMALA D. HARRIS, CALIFORNIA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

VIA ELECTRONIC TRANSMISSION

May 20, 2020

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Ave., NW
Washington, DC 20530

The Honorable Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528

Dear Director Wray and Director Krebs:

We write you today regarding a recent joint notice issued by the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Agency (CISA). This notice alerted American companies and research institutions about attempts by hackers affiliated with the Chinese government to target and steal intellectual property.

This announcement is alarming and we appreciate you notifying the public of this ongoing threat. While any government sponsored hacking of American companies is a cause for concern, it is especially troublesome that the Chinese government would target companies developing vaccines and treatments for the novel coronavirus.

According to the notice, these hacks jeopardized the delivery of “secure, effective, and efficient treatment option[s].” Any action that affects the development of treatment options—including attempted theft of American intellectual property—is a threat to our health, economic recovery, and national security. It is absolutely unacceptable for Chinese government affiliated hackers to attempt to steal or disrupt important research from companies and institutions who are developing essential diagnostics, cures, and treatments.

We wish to reiterate the request you made for any American companies or research institutions developing COVID-19 related intellectual property to take advantage of resources offered by CISA to prevent potential cyber intrusions. We hope that any company or institution that believes it is or was a target will report the intrusion to the FBI without delay.

We are confident that the FBI, CISA, and other involved federal agencies are working tirelessly to prevent attacks such as this. We are grateful to the dedicated agents and staff who are part of this effort, and we wish to support you in every possible way in these efforts.

Accordingly, we ask that you answer the following questions in a classified briefing with our staff by no later than June 20, 2020:

1. What additional statutory tools or authorities do your agencies require to more effectively combat state-sponsored hacking of American companies?
2. What additional financial resources or appropriations do you require in order to prevent and investigate further attempted thefts and intrusions?
3. What steps are your agencies taking—besides the recently published notice—to inform American companies or research institutions about the threats posed by Chinese hackers? In addition, what steps are you taking to help companies and research institutions increase their cybersecurity and prevent further intrusions?

Thank you for your prompt attention to this matter. Please know that as you continue to combat state sponsored hacking and the theft of American intellectual property we stand ready and willing to assist you. If you have any questions, please do not hesitate to contact us.



Thom Tillis
United States Senator

Sincerely,



Richard Blumenthal
United States Senator



John Cornyn
United States Senator



Ben Sasse
United States Senator



Comparison of COVID-19 Contact Tracing Bills

	COVID–19 Consumer Data Protection Act of 2020 (Wicker)	Public Health Emergency Privacy Act (Blumenthal/Warner)	Exposure Notification Privacy Act (Cassidy/Cantwell)	Key Differences Between Bills
Covered Entities	<p>Any business subject to the FTC Act (plus common carriers and nonprofits) that collects, processes or transfers “covered data” or determines the means of collecting, processing or transferring “covered data.”</p> <p><u>Exclusions</u> A service provider.¹</p>	<p>Any entity (including a government entity) that (i) collects, uses, or discloses emergency health data electronically or by wire or radio; or (ii) that develops or operates a website or application for the purpose of contact tracing or otherwise responding to the COVID–19 public health emergency (“PHE”).</p> <p><u>Exclusions</u> (1) a health care provider²; (2) a person engaged in a de minimis collection or processing of emergency</p>	<p>Applies primarily to operators of an “automated exposure notification service” (“AENS”), which is (1) any website, application or online service specifically designed or marketed for the purpose of automatically notifying an individual exposed to an infectious disease, and (2) that is covered by the FTC Act or a common carrier or nonprofit entity. Certain provisions apply to their service providers⁴ and</p>	<p>All are limited to entities that process COVID-19 (or in the case of Cassidy/Cantwell, any infectious disease) data, but Blumenthal/Warner includes government entities other than PHAs (other two bills don’t). Blumenthal/Warner specifically excludes certain health care providers and HIPAA entities (other two bills don’t although Wicker bill excludes PHI), but requires</p>

¹ A “service provider” is an entity that collects, processes or transfers covered data to perform services for a covered entity to which it is not related.

² “Health care provider” is defined as an “eligible health care provider” in Title VIII of division B of the CARES Act, which means “public entities, Medicare or Medicaid enrolled suppliers and providers, and such for-profit entities and not-for-profit entities not otherwise described in this proviso as the Secretary may specify, within the United States (including territories), that provide diagnoses, testing, or care for individuals with possible or actual cases of COVID– 19.”

⁴ A “service provider” is any entity, other than a platform operator, that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, a platform operator, an operator of an

		<p>health data; (3) a service provider³; (d) a person acting in their individual or household capacity; or (e) a public health authority.</p> <p>Requirements do not apply to HIPAA covered entities and business associates, but within 30 days of enactment HHS is to issue guidance applying similar requirements to HIPAA covered entities and business associates, but must avoid duplication and not include a requirement if already required by HIPAA.</p>	<p>“platform operators” (i.e., entities that facilitate the provision of an AENS).</p> <p><u>Exclusions</u> An operator of an AENS excludes a public health authority (“PHA”)</p>	<p>that HHS to issue guidance applying similar requirements to HIPAA entities.</p> <p>Blumenthal/Warner does not apply to an entity that collects data non-electronically and Cassidy/Cantwell is further limited to entities that operate an AENS, their service providers and platform operators.</p>
Covered Data	<p>Precise geolocation data, proximity data, a persistent identifier⁵, and personal health information⁶ of an individual.</p> <p><u>Exclusions</u> (1) aggregated data, (2) business contact information,⁷ (3) de-identified data, (4) employee screening</p>	<p>Emergency health data (“EHD”), which means data linked to or reasonably linkable to an individual or device that concerns the COVID–19 PHE. It includes geolocation, proximity, demographic, contact and any other data collected from a personal device.</p> <p><u>Exclusions</u></p>	<p>Any data (1) linked or reasonably linkable to an individual or to a device linked to or reasonably linkable to an individual, and (2) that is collected or processed in connection with an AENS. Does not include aggregate data (which is defined to require that the AENS use the data only</p>	<p>Wicker does not apply to business contact, employment-related or publicly available data and also excludes PHI from personal health information (other two bills don’t have these exclusions).</p> <p>While Wicker bill is not limited to data concerning the</p>

AENS or a PHA, but only to the extent that such processing or transfer relates to the performance of such service or function.

³ A “service provider” is a person that receives, maintains, or transmits personal health information for the sole purpose to conduct business activities on behalf, for the benefit, and under instruction of the covered entity, but excludes a person that develops or operates a website or app for purposes of contact tracing or otherwise responding to the COVID–19 PHE.

⁵ A “persistent identifier” means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier.

⁶ “Personal health information” means genetic information or information relating to the diagnosis or treatment of past, present, or future physical, mental health, or disability of the individual, and that identifies, or is reasonably linkable to, the individual.

⁷ “Business contact information” means information related to an individual’s business position name or title, business telephone number, business address, business email address, and other similar business information, provided that such information is collected, processed, or transferred solely for purposes related to such individual’s professional activities.

	<p>data⁸ and (5) publicly available information. Personal health information excludes protected health information (PHI) and education records subject to FERPA.</p> <p>An “individual” excludes an employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of a covered entity permitted to enter a physical site of operation of the covered entity.</p>	<p>Manual contact tracing and case investigation by public health authorities or their agents.</p>	<p>for public health purposes).</p>	<p>COVID-19 PHE or infectious disease exposure (as are the other two bills), its key provisions apply only during the COVID-19 PHE.</p> <p>While none of the bills apply to de-identified or aggregate data, by its definition of “aggregate data”, Cassidy/Cantwell limits the use of this data to public health purposes.</p>
<p>Prohibited Uses and Disclosures</p>		<p>May not disclose EHD to a government entity that is not a public health authority or for any purpose other than good faith public health purposes in direct response to exigent circumstances.</p> <p>May not collect, use or disclose EHD for a purpose not authorized by the bill, including (1) for commercial advertising and e-commerce; (2) for employment, finance, credit, insurance, housing, or education opportunities in a discriminatory manner or that otherwise makes opportunities unavailable on the basis of EHD or (3)</p>	<p>An operator of an AENS (1) cannot do so except in collaboration with a PHA; (2) may not collect, process or disclose a diagnosis of an infectious disease unless it is confirmed by a PHA or health care provider; (3) may not engage in deceptive acts in connection with the service.</p> <p>An operator of an AENS may not: (1) collect more than the minimum necessary data for the public health purpose or collect the data for a commercial purpose; (2) transfer the data except to:</p>	<p>AS long as affirmative express consent of individual is obtained, Wicker has no explicit prohibitions.</p> <p>Blumenthal/Warner and Cassidy/Cantwell prohibits use of EHD for unrelated purposes, including e-commerce or commercial purposes, but both include a broad exception for research (see below).</p> <p>Cassidy/Cantwell allows operation of the AENS only in collaboration with a PHA.</p>

⁸ “Employee screening data” means data of employees or other personal collected, processed or transferred by a covered entity for purposes of determining, for purposes related to the COVID-19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity.

		<p>segregating, discriminating or making unavailable places of public accommodation except for a lawful public health purpose.</p> <p>A government entity may not, and a covered organization may not knowingly facilitate the use of EHD to, or an individual’s decision whether to participate in a program collecting EHD to, restrict, deny or interfere with an individual’s right to vote. Individual’s may bring a civil action in federal court for appropriate relief against a government entity that violates this prohibition.</p>	<ul style="list-style-type: none"> • notify the individual of a potential exposure; • to a PHA for public health purposes related to an infectious disease; • to a service provider for limited purposes (see below); or • to exercise or defend a legal claim. <p>Data also may not be transferred to an executive agency except in connection with enforcing the bill or a for a public health purpose</p>	
Research		Does not prohibit public health or scientific research associated with the COVID–19 PHE by a public health authority, a 501(c)(3) nonprofit, an institution of higher education, or research, development, manufacture, or distribution of a drug, biological product, or vaccine that relates to a disease associated with the PHE.	Above restrictions do not prohibit collection or processing of data to carry out human subjects’ research or research for a drug or vaccine related to the infectious disease.	Blumenthal/Warner carve-out for research is limited to research associated with the COVID-19 PHE, whereas Cassidy/Cantwell research carve-out also includes any human subject research.
Prior Notice and Consent	During COVID-19 public health emergency (the “PHE”), covered entities must (obtain the individual’s affirmative consent to do for a covered purpose, and (3) publicly commit to not collecting, processing or transferring covered data	Must obtain the individual’s prior affirmative express consent before collecting, using or disclosing EHD unless it is for the sole purpose of (i) protecting against malicious, fraudulent, or illegal activity; or to detect or	Individuals must provide prior affirmative express consent to enroll in the AENS, and may choose whether to have a confirmed diagnosis processed as part of the AENS.	All require affirmative express consent prior to collection of data, but Wicker and Blumenthal/Warner have limited exceptions, with the Wicker bill exceptions being

	for any purpose other than a covered purpose <u>unless</u> (1) necessary to comply with the bill or other applicable laws; (2) necessary to carry out operational or administrative tasks in support of a covered purpose; or (3) the individual gives affirmative express consent for that purpose.	respond to security incidents or threats; or (ii) if compelled to do so by a legal obligation		potentially a little broader (in allowing use for operational or administrative tasks to support a covered purpose). Cassidy/Cantwell allows a partial consent in that individuals may choose whether or not their diagnosis information is included. Affirmative express consent under Cassidy/Cantwell requires a description “of each act or practice for which the individual’s consent is sought.”
Consent Revocation	During the COVID-19 PHE, must permit the individual to revoke their consent and must stop collecting, processing or transferring the data for a covered purpose as soon as practicable but no later than within 14 days of receipt of the revocations or must de-identify it.	Must provide an effective mechanism for an individual to revoke their consent and must stop collecting, using and disclosing their EHD as soon as practicable but no later than within 15 days after receipt of revocation. Must also destroy or render the EHD not linkable to the individual within 30 days of receipt of revocation. Must destroy EHD in a way that is impossible or demonstrably impracticable to identify the individual	Individuals must be able to withdraw their consent.	Under Wicker and Blumenthal, there is no revocation does not require deletion of data as long as it is de-identified. Cassidy/Cantwell is silent on effect of revocation, but individuals have a separate right to request deletion of their data at any time.
Privacy Policy	Within 14 days after enactment and during PHE, must publish a privacy policy and disclose it in a clear and	Must provide a clear and conspicuous privacy notice at or prior to point of collection of EHD that explains purposes for	An operator of an AENS and its platform operator must make a privacy policy readily and persistently	All require privacy notices, with Cassidy/Cantwell being the most granular in requiring

	<p>conspicuous manner to an individual prior to or at point of collection of their covered data and to the public. Must include categories of recipients of covered data, and a description of the covered entity’s retention and security practices.</p>	<p>which the data is collected, categories or recipients, the organization’s data retention and security practices, how individuals may exercise their rights and how to contact the FTC to file a complaint.</p>	<p>available that provides a detailed and accurate representation of their data collection activities related to the AENS, including (1) each category of data collected and the purposes for which it is collected; (2) a detailed description of any data transferred, the purpose of the transfer and identify the recipient of the data; (3) its data minimization, retention and security policies; and (4) how individuals can exercise their rights under the bill and contact information. The notice must be provided in all languages the service or platform is provided.</p> <p>An AENS operator must also publish guidance for the public on (1) the functionality of the service, how to interpret the notifications, including any limitation on the accuracy or reliability of the exposure risk; and (2) measures of the effectiveness of the service, including adoption rates.</p>	<p>the notice to “identify the recipient” of the data, as well as provide information on the functionality and effectiveness of the service (including adoption rates), and the accuracy and reliability of the data.</p>
<p>Public Reporting/ Public Reporting</p>	<p>During PHE, must provide a public report within 30 days of enactment and every 60 days thereafter of (1) the number of individuals in aggregate whose data it</p>	<p>A covered organization that collects EHD of at least 100,000 individuals must provide a public report every 90 days of the number of individuals in aggregate terms whose</p>	<p>Requires the Privacy and Civil Liberties Oversight Board (“PCLOB”) to issue a report assessing the impact on privacy and</p>	<p>Wicker and Blumenthal/Warner require periodic public reporting of data collection, whereas Cassidy/Cantwell</p>

	<p>has collected, processed or transferred, (2) the categories of data collected, processed or transferred and the purposes for which each category of covered data was collected, processed or transferred, and (3) for transferred covered data, to whom it was transferred.</p>	<p>data it has collected (to the extent practicable), the purposes for collection and the categories of third parties to whom disclosed</p> <p>HHS, in coordination with the US Commission on Civil Rights and the FTC must provide a report to Congress no sooner than 9 months or later than 12 months after enactment (and annually thereafter until 1 year after termination of the PHE) that examines the civil rights impact of the collection, use, and disclosure of health information in response to the COVID-19 PHE, including recommendations on preventing and addressing undue or disparate impact, segregation, discrimination, or infringements of civil rights in the collection and use of health information, including during a national health emergency.</p>	<p>civil liberties of government activities taken to respond to the COVID-19 public health emergency no later than 180 days after enactment and also after other public health emergencies.</p>	<p>requires public guidance on how the service operates.</p> <p>Blumenthal/Warner requires reporting to Congress and Cassidy/Cantwell requires oversight reporting by the PCLOB.</p>
<p>Data Deletion</p>	<p>Must delete or de-identify the data when no longer used for a covered purpose or needed to comply with law or establish or defend a legal claim.</p>	<p>May not use or retain EHD after the later of (i) the end of the PHE declared by HHS; (ii) the end of a PHE declared by a state governor, or (iii) 60 days after collection. These requirements do not supersede requirements under the Privacy Act, HIPAA or other federal or state medical record retention, privacy or other requirements.</p>	<p>Data must be deleted: (1) at the request of the individual; (2) within 30 days of collection or on a rolling basis or in accordance with standards published by a PHA. This also applies to data held by a service provider, but does not prohibit the retention of data for public health research.</p>	<p>Wicker does not provide explicit timeframes by which data must be deleted, whereas Blumenthal/Warner and Cassidy/Cantwell include certain parameters.</p> <p>Cassidy/Cantwell also requires deletion at the request of the individual, and requires deletion by service providers, but has an explicit carve-out of any deletion</p>

				requirement for public health research.
Data Accuracy	Must take reasonable measures to ensure accuracy of covered data collected for a covered purpose and provide individuals with an effective mechanism to report inaccuracies.	Must take reasonable measures, where possible, to ensure the accuracy of EHD and provide an effective mechanism for an individual to correct inaccurate information	No explicit requirements, but must provide public guidance on the accuracy and reliability of the “exposure risk”	Cassidy/Cantwell has no requirement to take measures to ensure accuracy of data, whereas other two bills do.
Discrimination		Must adopt reasonable safeguards to prevent unlawful discrimination on the basis of EHD.	It is unlawful to discriminate or fail to make available any place of public accommodation based on covered data or an individual’s choice to use or not to use an AENS.	Wicker has no explicit provision prohibiting discrimination, whereas the other two bills do.
Data Minimization	During PHE, must limit covered data collected, processed or transferred for a covered purpose to what is reasonably necessary, proportionate and limited to carry out that purpose. The FTC is to issue guidelines recommending best practices for this purpose within 30 days of enactment.	May only collect, use, or disclose EHD that is necessary, proportionate, and limited for a good faith public health purpose, including a service or feature to support that purpose.	May not collect or process any covered data beyond the minimum amount necessary to implement an AENS for public health purposes	All limit data collection to that needed to carry out the public health purpose, with Cassidy/Cantwell language being the tightest and Wicker requiring the FTC to issue guidance on this.
Service Providers	Not covered	Subject to same security requires as a covered entity	When a service provider has actual knowledge that an AENS operator or PHA has violated the requirements of the bill, it must notify the AENS operator or PHA. Covered data may only be transferred to a service provider, by contract, to: (A) perform system maintenance, debug	Wicker and Blumenthal largely carve-out service providers, whereas Cassidy/Cantwell imposes several affirmative obligations on service providers, including to notify the operator of the AENS and PHA of their violations known to the service provider, to delete data, and to provide breach notification. It also

			<p>systems, or repair any error to ensure the functionality of the AENS; or</p> <p>(B) detect or respond to a security incident, provide a secure environment, or maintain the safety of the AENS.</p> <p>Service providers are subject to same data deletion requirements as covered entities.</p>	explicitly limits the purposes for which covered data may be shared with a service provider.
Security	During the PHE, covered entities must implement physical, technical and administrative safeguards to protect covered data	Must establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data	Must implement security practices consistent with standards generally accepted by information security experts. These must include: (1) risk and vulnerability assessments, including testing systems for monitoring the security of covered data; and (2) taking mitigation and corrective actions to address the risks, and (3) notifying individuals and the FTC in the event of a breach, and requiring service providers to notify the AENS operator immediately of any security breaches they discover.	All require security measures, with Cassidy/Cantwell being the most granular and also including security breach notification requirements.
Enforcement	By FTC or State attorneys general	By the FTC or State attorneys general	By FTC or state attorneys general	

Private Right of Action		<p>An individual may bring a civil action for violations and the court may award between \$100-\$1000 per negligent violations and between \$500-\$5000 for reckless or intentional violations, as well as reasonable attorney fees, litigation costs and other appropriate relief. Any violation is deemed to be a concrete and particularized injury in fact.</p> <p>No pre-dispute arbitration agreement or pre-dispute joint action waiver will be valid or enforceable with respect to a dispute under the bill.</p>	<p>Does not preempt or supplant any Federal or State common law right or remedy, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability or any other legal theory of liability under any Federal or State common law, or any State statutory law.</p>	<p>Wicker has no private right of action, whereas both Blumenthal/Warner and Cassidy/Cantwell would allow a private right of action, with Blumenthal/Warner including specified statutory damages and deeming any violation to be an injury in fact.</p>
Preemption	<p>Preempts FCC regulations with respect to collection, processing or transfer of covered data for a covered purpose except with respect to 911 and emergency lines of hospitals, medical providers, fire departments or law enforcement.</p> <p>Also preempts state laws to the extent they relate to the collection, processing or transfer of covered data for a covered purpose</p>	<p>Does not preempt or supersede any Federal or State law or regulation, or limit the authority of the FTC or HHS under any other provision of law.</p>	<p>Does not preempt, displace, or supplant any State law, rule, or regulation.</p>	<p>Wicker preempts other related laws, whereas Blumenthal/Warner explicitly preserves Federal and State laws, and Cassidy/Cantwell preserves state laws.</p>
Effective Date	<p>Upon enactment</p>	<p>Within 30 days of enactment (except as specified in the bill for specific regulations to be issued). In addition, upon enactment, but within 7 days after enactment the FTC must initiate, and with 45 days after</p>	<p>Effective on enactment</p>	<p>Wicker and Cassidy/Cantwell are prospective only, whereas Blumenthal/Warner would require regulations to apply the requirements to data collected before</p>

		enactment must complete, rulemaking to apply the same requirements to EHD collected by covered organizations before the date of enactment to the degree practicable.		enactment to the extent practicable.
--	--	--	--	--------------------------------------

EXPOSURE NOTIFICATION PRIVACY ACT

Topline Message: Exposure notification apps can be a useful tool in combatting covid, however- 1) These methods only work if a significant amount of people use them
2) People will only use these apps if they trust them
3) Polls show people [do not trust them](#)
4) So, to achieve the capability of this public health tool, we must create guidelines to ensure individual privacy is protected. That is the purpose of this bill.

One-page Summary:

The Primary Role of Public Health Authorities & Licensed Health Care Providers

- The Act requires online exposure notification services to be operated by public health authorities or operated in collaboration with a public health authority. Independent exposure notification systems, created without direction from public health authorities, would be prohibited.
- The Act requires that online exposure notification services only process medical diagnoses of COVID-19 to ensure that the notifications individuals receive are accurate.

Ensuring Individuals' Rights

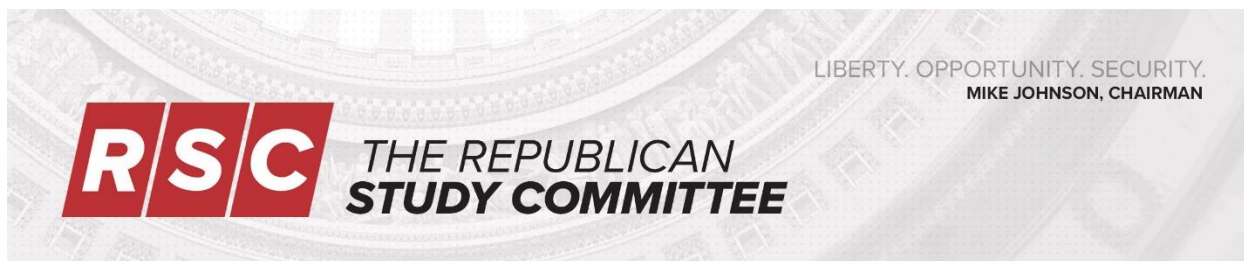
- The Act empowers individuals to control their participation in an online exposure notification service; individuals' consent must be freely-given and anyone can withdraw at any time.
- The Act allows participants in an online exposure notification system to have their data deleted at any time.
- The Act makes it unlawful to make unavailable to an individual, any place of public accommodation based solely on data collected or processed through an exposure notification online service.

Data Restrictions to Preserve Privacy

- The Act prohibits operators of exposure notification online services from collecting or using data beyond what is necessary to implement the exposure notification service. They are prohibited from processes and collecting data for any commercial purpose.
- The Act creates strong cybersecurity safeguards, requiring operators of exposure notification online services to conduct vulnerability assessments and take preventive and corrective action to protect participants' data.
- The Act requires the automatic deletion of participants' data every 30 days. Allowances are made for public health research.

Strong Enforcement

- The Act empowers the Federal Trade Commission and State Attorneys General to pursue violators.



RSC Backgrounder: COVID-19 “Testing, Tracing, and Treatment”

This backgrounder will discuss the latest developments, highlight Executive Branch actions, and underscore conservative concerns with policy options related to COVID-19 testing, tracing, and treatment.

Understanding the policy landscape surrounding testing, tracing, and treatment is critical as these issues will assume an important aspect in future pandemic-related legislation. In her weekly press conference on May 7th, before the House considered and passed the HEROES Act, Speaker Nancy Pelosi stressed the importance of the “the T’s”: testing, tracing, and treatment.^{1,2} Senate Majority Leader McConnell has also acknowledged the strong possibility of Congressional consideration of a fifth pandemic-related bill within the next month.³ While the Left and the Right have both suggested building the public and private response around testing, tracing, and treatment, a number of notable differences have emerged with respect to proposals touching on these topics.^{4,5}

In order to efficiently reopen the country while simultaneously preparing for a potentially dangerous second wave, quickly learning from mistakes and successes in America and abroad is critical.⁶ The federal government has been at its most effective when it has streamlined and simplified its complicated and excessive regulatory tendencies. While early warnings to ramp up testing capabilities were not heeded, once the Centers for Disease Control streamlined the Emergency Use Authorization process, removing its burdensome requirements from the equation, rapid diagnostic testing capabilities were quickly approved.⁷ These measures followed on successful regulatory practices seen in other countries. In South Korea, for example, testing efficacy requirements were

¹ “Transcript of Pelosi Weekly Press Conference Today.” *Speaker Nancy Pelosi*, 7 May 2020, www.speaker.gov/newsroom/5720-2.

² H.R. 6800, 116th Congress

³ Jordain Carney. “McConnell: Talking about Fifth Coronavirus Bill ‘in the next Month or so’.” *The Hill*, 26 May 2020, www.thehill.com/homenews/senate/499503-mcconnell-talking-about-fifth-coronavirus-bill-in-the-next-month-or-so.

⁴ Erin Simpson and Adam Conner. “Digital Contact Tracing To Contain the Coronavirus.” *Center for American Progress*, 22 Apr. 2020, www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-tracing-contain-coronavirus/.

⁵ Scott Gottlieb et al. “National Coronavirus Response: A Road Map to Reopening.” *American Enterprise Institute*, 28 Mar. 2020, www.aei.org/wp-content/uploads/2020/03/National-Coronavirus-Response-a-Road-Map-to-Recovering-2.pdf.

⁶ Lena H. Sun. “CDC Director Warns Second Wave of Coronavirus Is Likely to Be Even More Devastating.” *The Washington Post*, 21 Apr. 2020, www.washingtonpost.com/health/2020/04/21/coronavirus-secondwave-cdcdirector/.

⁷ Luciana Borio and Scott Gottlieb. “Opinion | Act Now to Prevent an American Epidemic.” *The Wall Street Journal*, 28 Jan. 2020, www.wsj.com/articles/act-now-to-prevent-an-american-epidemic-11580255335.

relaxed and testing was not stringently vetted, allowing for overall capabilities to be put in place rapidly.

These lessons illuminate measures key to returning to normalcy. Leading scholars have laid out various plans which Congress may consider. Experts largely agree that ensuring tools such as diagnostic testing, serologic testing, and tracing capabilities are available to the American public is vital.⁸ While a vaccine will ultimately be needed for a complete return to normalcy, streamlining and fast-tracking antiviral therapies may serve as a bridge to that end goal. In combination, these tools will be critical in both re-engaging the American economy and allowing it to overcome the possibility of a second wave in the fall.⁹

Testing

There are two major variants of COVID-19 testing: 1) diagnostic testing for active infections and; 2) serological testing—or testing for antibodies. Testing for active infections, more prevalently discussed in the media, can be further stratified into three different purpose: 1) diagnostic testing to confirm viral infections in symptomatic individuals; 2) diagnostic testing for tracking contacts of those infected; 3) broad-based surveillance testing. Within these parameters, testing for COVID-19 has continued to be a focal point of every debate regarding fully reopening the American economy.

Diagnostic Testing

H.R. 266, the Paycheck Protection Program and Health Care Enhancement Act, required the Secretary of Health and Human Services (HHS) to create a COVID-19 strategic testing plan.¹⁰ That plan, delivered to Congress on May 24th, provides a stark contrast between the Administration's state-centered, localized approach to ramping up testing capabilities, and the top-down, centralized approach offered by Speaker Pelosi in the HEROES Act.¹¹ As the plan notes, United States' testing capabilities have exponentially increased over the course of the past two months. While critics have claimed the report's initial benchmark of 300,000 tests per day is too low to sufficiently contain the virus, the report also notes that the number is growing steadily at 25-30% each week and 300,000 tests per day will be surpassed.¹² Indeed, recent per day totals have surpassed 500,000 and continue that trajectory.¹³

Some experts and many on the Left believe that in order to ensure a safe reopening, testing must increase by orders of magnitude and must expand beyond diagnostic testing of symptomatic individuals. According to the Safra Center for Ethics at Harvard University, in order to “control the

⁸ Chad Terhune. “SPECIAL REPORT-How Korea Trounced U.S. in Race to Test People for Coronavirus.” *Reuters*, Thomson Reuters, 19 Mar. 2020, www.reuters.com/article/health-coronavirus-testing/special-report-how-korea-trounced-u-s-in-race-to-test-people-for-coronavirus-idUSL4N2BC1PH.

⁹ Strohman, Andrew, et al. “The Bridge to a Vaccine: Antiviral and Antibody Therapies for COVID-19.” *AAF*, 22 Apr. 2020, www.americanactionforum.org/insight/the-bridge-to-a-vaccine-antiviral-and-antibody-therapies-for-covid-19/.

¹⁰ P.L. 116-139

¹¹ U.S. Department of Health and Human Services, Report to Congress, COVID-19 Strategic Testing Plan, 24 May. 2020

¹² Apoorva Mandavilli and Catie Edmondson. “‘This Is Not the Hunger Games’: National Testing Strategy Draws Concerns.” *The New York Times*, The New York Times, 25 May 2020, www.nytimes.com/2020/05/25/health/coronavirus-testing-trump.html.

¹³ “US Historical Data.” *The COVID Tracking Project*, www.covidtracking.com/data/us-daily.

disease,” conducting up to 100 million tests each day may be necessary.¹⁴ Observers may note that the very same experts who now call for millions of tests each day just last month were calling for 500,000, a rate the country surpassed on June 5th.¹⁵ In the Safra Center’s most optimistic estimates, 1-10 million tests would suffice. In contrast, the American Enterprise Institute suggests 750,000 tests per week, a milestone already surpassed, could be sufficient when paired with sufficient contact tracing capacity.¹⁶

Many conservatives may note that testing capability should not be used as the sole barometer for reopening the nation’s economy. Focusing on overall testing numbers alone would disregard many other relevant considerations. Such a barometer completely overlooks many of the unseen healthcare costs of the current shutdowns.¹⁷ Cancer diagnoses are down, and some Americans with cancer are forgoing treatment because of the pandemic.¹⁸ As many as 40% of Americans who experience an acute stroke may be avoiding emergency care, and new parents worldwide are forgoing routine immunizations.¹⁹ Further, such a broad focus on testing itself ignores the need for prioritization and focus. As a report released by House Energy & Commerce Committee Republicans (E&C report) notes, nursing homes and other congregate living centers account for more than 40 percent of COVID-19 deaths.²⁰ “Smart testing,” which would focused testing on such facilities and other high-risk populations, would yield more actionable data for reopening. Finally, while overall case counts are indeed high, many conservatives note that is possibly due to more prevalent overall testing, as deaths per capita in America are on par with much of Europe.

Whether the top-down, bureaucratic national testing regime pushed by the Left, or the Administration’s approach of leveraging Federal resources to support state testing systems, increasing testing capacity and rapidity will remain a central tenet to every pandemic response plan. Bipartisan approaches to supporting local diagnostic and point-of-care testing capacity will likely be

¹⁴ Divya Siddarth and E. Glen Wey. “Why We Must Test Millions a Day.” *Edmond J. Safra Center for Ethics*, Harvard University, 8 Apr. 2020, www.ethics.harvard.edu/files/center-for-ethics/files/white_paper_6_testing_millions_final.pdf.

¹⁵ Rob Stein et al. “U.S. Coronavirus Testing Still Falls Short. How’s Your State Doing?” *NPR*, 7 May 2020, www.npr.org/sections/health-shots/2020/05/07/851610771/u-s-coronavirus-testing-still-falls-short-hows-your-state-doing; Ashish K Jha et al. “Why We Need at Least 500,000 Tests per Day to Open the Economy - and Stay Open.” *Harvard Global Health Institute*, 7 May 2020, <https://globalepidemics.org/2020/04/18/why-we-need-500000-tests-per-day-to-open-the-economy-and-stay-open/>.

¹⁶ Gottlieb et al.

¹⁷ Scott W. Atlas et al. “The COVID-19 Shutdown Will Cost Americans Millions of Years of Life.” *TheHill*, 26 May 2020, www.thehill.com/opinion/healthcare/499394-the-covid-19-shutdown-will-cost-americans-millions-of-years-of-life.

¹⁸ Avinash G. Dinmohamed et al. “Fewer Cancer Diagnoses during the COVID-19 Epidemic in the Netherlands.” *The Lancet*, 30 Apr. 2020, [https://doi.org/10.1016/S1470-2045\(20\)30265](https://doi.org/10.1016/S1470-2045(20)30265); Brian P. Dunleavy “Cancer Patient Care Disrupted by COVID-19 Pandemic.” *UPI*, 1 Apr. 2020, www.upi.com/Health_News/2020/04/01/Cancer-patient-care-disrupted-by-COVID-19-pandemic/7251585762174/.

¹⁹ Damian McNamara. “COVID-19 Cuts Stroke Cases Nearly 40% Nationwide.” *Medscape*, 12 May 2020, www.medscape.com/viewarticle/930374; Wakil Kohsar. “Coronavirus Forcing Parents to Skip Kids’ Vaccinations: UNICEF.” *Barron’s*, 26 Mar. 2020, www.barrons.com/news/coronavirus-forcing-parents-to-skip-kids-vaccinations-unicef-01585222805.

²⁰ “COVID-19 Second Wave Preparedness Part 1: Testing & Surveillance.” *House Energy and Commerce Committee*, Republicans, 2 June 2020, https://republicans-energycommerce.house.gov/wp-content/uploads/2020/06/COVID-19-Second-Wave-Report_Testing-Surveillance_FINAL.pdf.

among those receiving consideration in further pandemic response legislation.²¹ While conservatives may consider some federal support as within the parameters of a targeted, temporal response to the pandemic, conservatives should be vigilant about moving goalposts and excessive federal spending.

Serological testing

An antibody test, also known as a serology test, detects whether an individual has developed antibodies in their blood against SARS-CoV-2, the virus that causes COVID-19. While the antibodies, which typically develop one to three weeks after an individual is sick with COVID-19, indicate an immune response, it is not clear whether they ensure immunity to COVID-19, and if they do, how long such protection lasts. Generally, the existence of antibodies does provide some level of protection against viral reinfection.²² Additionally, more prevalent antibody testing will give a true scope of the pandemic's impact. As data from antibody testing accrues, mounting evidence points to widespread infection with a lower mortality rate.²³

As greater portions of the country reopen, some in Congress have broached the possibility of different forms of "immunity passports."²⁴ This would grant some sort of official recognition and reassurance to those individuals who have developed antibodies. In theory, this would allow a certain portion of the workforce which has had its safety confirmed to form the foundation of a reopening. Conservatives may have practical and ethical reservations with such an idea. For instance, while all testing discussed have relatively high failure rates, serological tests are particularly unreliable and often result in false positives. Many conservatives may also be resistant to a database that would be required to utilize serological testing in such a manner. Additionally, immunity passports could work to incentivize non-immune individuals to seek out infection. While such tools may prove effective for private businesses and localities, conservatives may be wary of potential abuse in the hands of the government.

Some conservatives have noted the significant benefits of widespread antibody testing itself. Greater utilization of serological testing as a tool would allow private entities and local jurisdictions to make more informed decisions as the country returns to normalcy. Recent evidence shows that even mild infection leads to the development of antibodies.²⁵ H.R. 266 appropriated \$25 billion to the Public Health and Social Services Emergency Fund, which, among other things, specifically authorized the expansion of serological testing capacity. The Administration is moving forward with national

²¹ "Lawmakers Introduce Legislation to Expand Coronavirus Testing Capacity and Accessibility." *Office of Representative Larry Buschon*, 27 May 2020, <https://buschon.house.gov/news/documentsingle.aspx?DocumentID=3881>.

²² "Test for Past Infection (Antibody Test)." *Centers for Disease Control and Prevention*, 23 May 2020, www.cdc.gov/coronavirus/2019-ncov/testing/serology-overview.html.

²³ Jon Hamilton. "Antibody Tests Point To Lower Death Rate For The Coronavirus Than First Thought." *NPR*, 28 May 2020, www.npr.org/sections/health-shots/2020/05/28/863944333/antibody-tests-point-to-lower-death-rate-for-the-coronavirus-than-first-thought.

²⁴ Tina Reed. "Emanuel: 'Immunity Passports' Could Help Open Economy, but Science Still Needed." *FierceHealthcare*, 12 May 2020, www.fiercehealthcare.com/practices/there-s-increasing-interest-idea-covid-19-immunity-passports-are-they-a-good-idea.

²⁵ Samira Fafi-Kremer, et al. "Serologic Responses to SARS-CoV-2 Infection among Hospital Staff with Mild Disease in Eastern France." *MedRxiv*, Cold Spring Harbor Laboratory Press, 1 Jan. 2020, www.medrxiv.org/content/10.1101/2020.05.19.20101832v2.

research priorities related to serological testing.²⁶ The E&C report released by Republicans also highlights the importance and various uses of serological testing, including potential use to manufacture convalescent plasma as a possible treatment, while denoting potential limitations. Democrats, however, have pushed back on the use of serological tests to inform easing of lockdowns, and called for greater regulation of their accuracy.²⁷

Contact Tracing

In recent weeks, America has seemingly turned the corner on COVID-19 testing.²⁸ As discussed above, leading experts point to ramping up diagnostic testing as a key pillar in the public health response to COVID-19. However, testing is not the sole solution to containing the virus and reopening the economy. Indeed, the testing goals set by leading think tanks are typically qualified by increased contact tracing regimes.

Contact tracing is the identification of individuals who may have come into contact with an infected individual, and the collection of relevant information about those contacts.²⁹ Contact tracing techniques generally include low-tech, case-by-case contact tracing, and digital contact tracing, which is typically used to augment case-by-case tracing. Digital contact tracing can further be delineated between a centralized, mandatory approach and a decentralized, voluntary, digital approach.

These approaches have been applied both at home and abroad.³⁰ In South Korea, while initial testing was integral to its rapid response to the coronavirus, its COVID-19 containment relied on mandatory and heavy-handed contact-tracing laws.³¹ These were put in place after the country's experience with the Middle East respiratory syndrome (MERS), allowing the country to utilize GPS phone tracking, CCTV, and credit card information to track and quarantine individual cases.³² Information about

²⁶ "NOT-CA-20-065: Request for Information (RFI): Strategy for Research in Coronavirus Serology Testing and Serological Sciences." *National Institutes of Health*, U.S. Department of Health and Human Services, <https://grants.nih.gov/grants/guide/notice-files/NOT-CA-20-065.html>.

²⁷ "Preliminary Findings of the Subcommittee's Coronavirus Antibody Testing Investigation." Memorandum to Democratic Members of the Subcommittee on Economic and Consumer Policy, House Committee on Oversight and Reform, Majority. Available here: <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/ECP%20Staff%20Report%20on%20Preliminary%20Findings%20of%20the%20Subcommittee%E2%80%99s%20Coronavirus%20Antibody%20Testing%20Investigation.pdf>

²⁸ Yael Halon. "Surgeon General Says US Has 'Turned the Corner' on Coronavirus Testing." *Fox News*, FOX News Network, 25 Mar. 2020, www.foxnews.com/media/surgeon-general-coronavirus-testing-turned-corner.

²⁹ "Contact Tracing." *World Health Organization*, www.who.int/news-room/q-a-detail/contact-tracing.

³⁰ O'Neill, Patrick Howell. "A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them." *MIT Technology Review*, 2 June 2020, www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

³¹ JSD Sangchul Park. "Privacy Controversies Around Information Technology–Based COVID-19 Tracing in South Korea." *JAMA*, American Medical Association, 2 June 2020, <https://jamanetwork.com/journals/jama/fullarticle/2765252?guestAccessKey=df9e7fb6-7c2d-42fb-9224-265469bf477e>.

³² Thompson, Derek. "What's South Korea's COVID Secret?" *The Atlantic*, 6 May 2020, www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/; Max S. Kim, et al. "Seoul's Radical Experiment in Digital Contact Tracing." *The New Yorker*, 17 Apr. 2020, www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing; Alexandra Sternlicht. "South Korea's Widespread Testing And Contact Tracing Lead To First Day With No New Cases."

these individuals is then published, sometimes enough information to make them identifiable. China has instituted similarly drastic, technologically-assisted methods to trace COVID-19 patients.³³ These policies, combined with zero-tolerance isolation of infected patients, has resulted in effective results, but may conjure a number of a civil liberty concerns.

Other countries, such as Singapore and Australia, have turned to similar utilization of app-based approaches to bolster their contact tracing systems. These countries encourage their citizens to download an app which then assists in monitoring the outbreak. However digital contact tracing requires high take-up in order to be effective. Singapore and Australia have both faced limited success due at least in part to citizens' privacy qualms.³⁴ Germany, while engaged in its own debate over contact tracing apps, has largely turned to case-by-case tracing.³⁵ The country, which has been praised for its response due to low infection and mortality rates, has hired a legion of contact tracers to follow up with patients individually.

To date, the United States has taken a decentralized, state-led approach to contact tracing, supported federally by funds appropriated through both the CARES Act and H.R 266. While every state has begun implementation of a contact tracing program, they have differed in form and scale. Texas, for example, has contracted with a private technology company to grow a contact tracing workforce.³⁶ South Carolina, which Dr. Anthony Fauci pointed to as a model for the rest of the country, instituted case-by-case contact tracing utilizing both private and public staff.³⁷ Whereas Texas uses an online system for Texans to self-report positive COVID-19 tests, South Carolina is one of three states that have announced plans to build an app using exposure notification technology made available by a private partnership between Apple and Google.³⁸

Forbes, Forbes Magazine, 30 Apr. 2020, www.forbes.com/sites/alexandrasternlicht/2020/04/30/south-koreas-widespread-testing-and-contact-tracing-lead-to-first-day-with-no-new-cases/.

³³ Paul Mozur, et al. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." *The New York Times*, 2 Mar. 2020, www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

³⁴ Liza Lin and Chong Koh Ping. "Singapore Built a Coronavirus App, but It Hasn't Worked So Far." *The Wall Street Journal*, Dow Jones & Company, 22 Apr. 2020, www.wsj.com/articles/singapore-built-a-coronavirus-app-but-it-hasnt-worked-so-far-11587547805; Josh Taylor. "How Did the CoviSafe App Go from Being Vital to Almost Irrelevant?" *The Guardian*, 23 May 2020, www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant.

³⁵ Luisa Beck Loveday Morris. "While U.S. Struggles to Roll out Coronavirus Contact Tracing, Germany Has Been Doing It from the Start." *The Washington Post*, 25 May 2020, www.washingtonpost.com/world/europe/contact-tracing-coronavirus-germany/2020/05/24/7e59a668-93c1-11ea-87a3-22d324235636_story.html; Tyson Barker. "Germany's Angst Is Killing Its Coronavirus Tracing App." *Foreign Policy*, 8 May 2020, www.foreignpolicy.com/2020/05/08/germany-coronavirus-contact-tracing-pandemic-app/.

³⁶ Jay Root and Jeremy Blackman. "Texas Signs \$295M Deal with MTX Group to Manage COVID-19 Contact Tracing Buildup." *Houston Chronicle*, 16 May 2020, www.houstonchronicle.com/politics/texas/article/news/article/Texas-signs-295M-deal-with-MTX-Group-to-manage-15275236.php.

³⁷ Jenny Meredith. "How Coronavirus Contact Tracing Works in a State Dr. Fauci Praised as a Model to Follow." *The Conversation*, 28 May 2020, www.theconversation.com/how-coronavirus-contact-tracing-works-in-a-state-dr-fauci-praised-as-a-model-to-follow-138757.

³⁸ Rachel Sandler. "Alabama, North Dakota And South Carolina To Debut Apple And Google's Covid-19 Contact Tracing." *Forbes*, 20 May 2020, www.forbes.com/sites/rachelsandler/2020/05/20/alabama-north-dakota-and-south-carolina-to-debut-apple-and-googles-covid-19-contact-tracing/.

Implications of Implementation

These approaches and considerations will likely form a foundation for Congressional debate. Implementation of contact tracing programs has differed on a state-by-state basis.³⁹ Various private and public collaborations are incorporating new features into mobile operating systems to allow for digital contact tracing.⁴⁰ Such systems, which would be hypothetically utilized by government health agencies, and contact tracing more generally, raise significant logistical, practical, and constitutional implications.

Storage of location data by tech companies is a top concern. This debate was a major focus of last month's "paper hearing" conducted by the Senate Committee on Commerce, Science, and Transportation.⁴¹ Given these privacy concerns, the exposure notification technology promoted by Google and Apple utilizes Bluetooth technology that does not record location data.⁴² Some critics have noted, however, that the tech giants' may hold too much power over the process and that Congress should step in.⁴³ Under current law, digital contact tracing is only governed by the Health Insurance Portability and Accountability Act (HIPAA) for certain "covered entities."⁴⁴ Democrats and Republicans have introduced competing proposals in the Senate related to the accumulation and use of tracing data.⁴⁵ Additionally, a bipartisan bill, the Exposure Notification Privacy Act, which deals specifically with digital contact tracing technology, was introduced last week.⁴⁶ Some have noted this language tracks closely with the policies already enacted by Apple and Google.⁴⁷ Leading conservatives have called for due process, freedom of association, and civil liberties to be protected

³⁹ "State Approaches to Contact Tracing during the COVID-19 Pandemic." *The National Academy for State Health Policy*, 29 May 2020, www.nashp.org/state-approaches-to-contact-tracing-covid-19/.

⁴⁰ Andy Greenberg. "How Apple and Google Are Enabling Covid-19 Bluetooth Contact-Tracing." *Wired*, 10 Apr. 2020, www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/; Lisa Stiffler. "UW and Microsoft Release Contact-Tracing App, Aiming to Battle COVID-19 While Preserving Privacy." *GeekWire*, 22 Apr. 2020, www.geekwire.com/2020/uw-microsoft-release-contact-tracing-app-aiming-battle-covid-19-preserving-privacy/.

⁴¹ "Enlisting Big Data in the Fight Against Coronavirus." *U.S. Senate Committee on Commerce, Science, & Transportation*, 16 Apr. 2020, www.commerce.senate.gov/2020/4/enlisting-big-data-in-the-fight-against-coronavirus.

⁴² Andy Greenberg. "Clever Crypto Could Protect Privacy in Covid-19 Contact-Tracing Apps." *Wired*, 8 Apr. 2020, www.wired.com/story/covid-19-contact-tracing-apps-cryptography/.

⁴³ Jeffrey Kahn and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. *Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance*. Johns Hopkins University Press, 2020. Project MUSE, [doi:10.1353/book.75831](https://doi.org/10.1353/book.75831).

⁴⁴ Carmel Shachar. "Protecting Privacy In Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork." *Health Affairs*, 19 May 2020, www.healthaffairs.org/doi/10.1377/hblog20200515.190582/full/.

⁴⁵ "To Protect Civil Liberties During COVID-19, Bennet Co-Sponsors the Public Health Emergency Privacy Act." *Office of Senator Michael Bennet*, 19 May 2020, www.bennet.senate.gov/public/index.cfm/press-releases?id=689EBA6C-C3D0-401A-B514-D2160EC5EB69; "Committee Leaders Introduce Data Privacy Bill." *U.S. Senate Committee on Commerce, Science, & Transportation*, 7 May 2020, www.commerce.senate.gov/2020/5/committee-leaders-introduce-data-privacy-bill.

⁴⁶ "Cantwell, Cassidy, and Klobuchar Introduce Bipartisan Legislation to Protect Consumer Privacy, Promote Public Health for COVID-19 Exposure Notification Apps: U.S. Senator Maria Cantwell of Washington." *Office of Senator Maria Cantwell*, 1 June 2020, www.cantwell.senate.gov/news/press-releases/cantwell-cassidy-and-klobuchar-introduce-bipartisan-legislation-to-protect-consumer-privacy-promote-public-health-for-covid-19-exposure-notification-apps.

⁴⁷ Bobbie Johnson. "The US's Draft Law on Contact Tracing Apps Is a Step behind Apple and Google." *MIT Technology Review*, 2 June 2020, www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/.

under any contact tracing program.⁴⁸ Public health experts, who have called for specific digital contact tracing legislation, have also sought similar protections for privacy.⁴⁹

Conservatives may also be skeptical of the cost of some of the measures being considered, as well as attempts to instate a national program mirroring those instituted abroad. The Democrat-led HEROES Act included \$75 billion for testing and tracing infrastructure, which is on top of the \$25 billion already appropriated in H.R. 266. Further, a leading Democrat proposal, H.R. 6666, the COVID-19 Testing, Reaching, And Contacting Everyone (TRACE) Act, would appropriate \$100 billion for the testing, tracing, monitoring and, also concerning to many conservatives, quarantining of infected individuals.⁵⁰ These appropriations far exceed the estimates of leading experts. The Center for Health Security at Johns Hopkins University pinned the cost of hiring the 100,000-person workforce it suggested at \$3.6 billion. A bipartisan group of public health leaders, including former FDA Commissioner Scott Gottlieb, suggested hiring 180,000 workers at a cost of \$12 billion.

Under any program, privacy and cost must be balanced with efficacy. As noted, national digital tracing apps have attained varying degrees of success. Many have been plagued by low take-up rates, which undermines the ability for technology to provide actionable results.⁵¹ Experts have noted that upwards of 80% of the population would have to use the app in order to be effective, which would only be possible if every American owning a smartphone used the app.⁵² Finally, some have expressed skepticism of the efficacy of contact tracing at this stage in the pandemic in any form.⁵³ A major reason for the successes in countries like Germany and South Korea, and in States like South Carolina, is that contact tracing was implemented there early with strong testing programs. Instead, more widespread use of serological testing to gain an understanding of the virus' existing path may yield more actionable data.⁵⁴

Treatments

While testing and contact tracing can certainly help mitigate the spread of the virus, a true return to normalcy will not happen while there is still potential asymptomatic transmission of SARS-CoV-2 with no significant advances in COVID-19 treatment.⁵⁵ In total, more than 70 clinical trials for vaccines and treatments have registered with the FDA. While taking place at a groundbreaking pace, successful development of a vaccine is still likely many months away.⁵⁶ In the interim, prophylactic

⁴⁸ Josh Withrow. "Contact Tracing: Strict Guidelines Are Needed to Prevent a ..." *FreedomWorks*, 8 May 2020, www.freedomworks.org/content/contact-tracing-strict-guidelines-are-needed-prevent-civil-liberties-nightmare.

⁴⁹ Kahn, *Digital Contact Tracing for Pandemic Response*

⁵⁰ H.R. 6666, 116th Congress

⁵¹ Zak Doffman. "Forget Apple And Google: Contact-Tracing Apps Just Dealt Serious New Blow." *Forbes*, 13 May 2020, www.forbes.com/sites/zakdoffman/2020/05/12/forget-apple-and-google-contact-tracing-apps-just-dealt-serious-new-blow/.

⁵² "Demographics of Mobile Device Ownership and Adoption in the United States." *Pew Research Center: Internet, Science & Tech*, Pew Research Center, www.pewresearch.org/internet/fact-sheet/mobile/.

⁵³ Yael Halon. "Dr. Scott Atlas Knocks Contract Tracing Push: 'It's the Improper Tool at This Point in This Infection'." *Fox News*, 8 May 2020, www.foxnews.com/media/dr-atlas-contact-tracing-coronavirus.

⁵⁴ Andrew Joseph. "The next Frontier in Coronavirus Testing: Identifying the Outbreak's Full Scope." *STAT*, 26 Mar. 2020, www.statnews.com/2020/03/27/serological-tests-reveal-immune-coronavirus/.

⁵⁵ Roman Wölfel, et al. "Virological Assessment of Hospitalized Patients with COVID-2019." *Nature News*, Nature Publishing Group, 1 Apr. 2020, www.nature.com/articles/s41586-020-2196-x.

⁵⁶ Carolyn Kormann, et al. "How Long Will It Take to Develop a Coronavirus Vaccine?" *The New Yorker*, 8 Mar. 2020, www.newyorker.com/news/news-desk/how-long-will-it-take-to-develop-a-coronavirus-vaccine.

and therapeutic treatments are seen as the best method to reduce the near term health impacts of COVID-19. The Trump administration recently launched Operation Warp Speed, utilizing \$10 billion directed through the CARES Act to accelerate “the development, manufacturing, and distribution of COVID-19 vaccines, therapeutics, and diagnostics (medical countermeasures).”⁵⁷

While two treatments, remdesivir and hydroxychloroquine, have garnered the most media attention, more than 20 drug companies have announced the development of various antibody and antiviral treatments.⁵⁸ Remdesivir, for example, is an antiviral therapy meant to block the virus from replicating. Antibody treatments work differently, aiming to artificially reproduce antibodies from people who have recovered from COVID-19, a type of treatment that could be used prophylactically to stave off infections. Also making headlines is a third possible approach touted by some scientists in which convalescent plasma is transfused from survivors directly into the infected.⁵⁹

Congress has already taken significant steps to accelerate COVID-19 treatments. The administration, too, has taken steps to streamline and hasten the typically slow bureaucratic processes surrounding drug development. In April, the National Institutes of Health (NIH) announced the Advancing COVID-19 Therapeutic Interventions and Vaccines (ACTIV) public-private partnership.⁶⁰ Through ACTIV, NIH is partnering with the Biomedical Advanced Research and Development Authority (BARDA), Centers for Disease Control and Prevention (CDC), and the FDA; other government agencies including the Department of Defense (DOD) and Department of Veterans Affairs (VA); the European Medicines Agency (EMA); and representatives from academia, philanthropic organizations, and more than 15 private biopharmaceutical companies.

The ACTIV partnership is designed to accelerate the preclinical and clinical trial process.⁶¹ Although Democrat’s have continuously called for centralized, bureaucratic, nationalized treatment development regimes, the ACTIV partnership has produced rapid results through decentralized coordination. By collaborating with private industry and streamlining the efforts of multiple agencies, a vaccine is on schedule to enter trials by July 1, 2020.

In concrete terms, Congress, ACTIV, and health policy leaders will have to balance various trade-offs in drug efficacy and safety. Many, across the spectrum of political affiliation, suggested the use of “Human Challenge Trials” to hasten the advancement of a potential vaccine.⁶² In such a trial, a patient would receive both the vaccine *and the virus*. Further, many conservatives have called for the FDA to

⁵⁷ “Trump Administration Announces Framework and Leadership for ‘Operation Warp Speed.’” *HHS.gov*, US Department of Health and Human Services, 15 May 2020, www.hhs.gov/about/news/2020/05/15/trump-administration-announces-framework-and-leadership-for-operation-warp-speed.html.

⁵⁸ “STAT’s Covid-19 Drugs and Vaccines Tracker.” *STAT*, 27 Apr. 2020, www.statnews.com/feature/coronavirus/drugs-vaccines-tracker/?utm_campaign=hp_widget.

⁵⁹ Jillian Kramer. “Coronavirus Antibody Therapies Raise Hopes-and Skepticism.” *Scientific American*, 29 May 2020, www.scientificamerican.com/article/coronavirus-antibody-therapies-raise-hopes-and-skepticism1/.

⁶⁰ “ACTIV.” *National Institutes of Health*, U.S. Department of Health and Human Services, www.nih.gov/research-training/medical-research-initiatives/activ.

⁶¹ Francis S. Collins. “Accelerating COVID-19 Therapeutic Interventions and Vaccines (ACTIV).” *JAMA*, 18 May 2020, www.jamanetwork.com/journals/jama/fullarticle/2766371?guestAccessKey=5defc755-e585-47e5-b79a-fee2ec2dd42b.

⁶² Daniel Klein. “Human Challenge Trials Are the Free Market.” *Mercatus Center*, 21 May 2020, www.mercatus.org/bridge/commentary/human-challenge-trials-are-free-market; Nir Eyal, et al. “Human Challenge Studies to Accelerate Coronavirus Vaccine Licensure.” *OUP Academic*, Oxford University Press, 31 Mar. 2020, <https://academic.oup.com/jid/article/221/11/1752/5814216>.

make experimental drugs and vaccines available to patients after Phase I trials have been completed.⁶³ Streamlining these processes, which can typically take roughly 12 years, will be critical to the development of treatments in a time sufficient to ensure economic recovery.⁶⁴

Drug Pricing

With significant government involvement, whether through the issuance of emergency use authorizations, funding, or clinical trial partnerships, renewed attention has been brought to the issue of drug pricing. While the issue had been a top concern for Congress in the months and years preceding the pandemic, recent developments will likely bring it to the fore once again. Several prominent left-leaning organizations and experts have pushed for the government to use “march-in” rights afforded by the Bayh-Dole Act of 1980 in order to seize patents and prevent “profiteering.”⁶⁵ While such an extreme measure, which has not been practiced since Bayh-Dole was enacted, may only appeal to the Left’s more radical base, provisions in the HEROES Act are consistent with long-held Democrat affinities for instituting price controls.

The development of one drug in particular, Gilead’s remdesivir, has garnered significant attention. As the drug has been shown to be at least modestly effective in accelerating recovery in COVID-19 patients, it was granted “emergency use authorization” by the FDA in late April. For its part, Gilead Sciences has agreed to donate its existing supply to treat COVID-19 patients at no cost. Other companies developing treatments and vaccines have taken similar steps.

Conservatives will be wary of attempts from the Left to assert financial control over private industry. Many conservatives have noted that Bayh-Dole, while including “march-in” rights, was primarily an attempt to incentivize private industry through the reform of intellectual property arising from at least partially federally funded research. Controlling private industry that partners with the federal government will only serve to discourage private companies from agreeing to shoulder the exorbitant costs of bringing a drug to market.⁶⁶ Instead of attempting to manipulate existing pro-innovation law to impose innovation-stifling price controls—which was never the intent of the law, according to former Sen. Bob Dole—conservatives has instead recognized the need to decrease the

⁶³ Benjamin Yeoh. “Regulators Could Allow Early Use of COVID-19 Vaccine or Treatment.” *Mercatus Center*, 21 May 2020, www.mercatus.org/publications/covid-19-crisis-response/regulators-could-allow-early-use-covid-19-vaccine-or-treatment.

⁶⁴ Gail A. Van Norman. “Drugs, Devices, and the FDA: Part 1: An Overview of Approval Processes for Drugs.” *Science Direct*, Elsevier, 25 Apr. 2016, www.sciencedirect.com/science/article/pii/S2452302X1600036X.

⁶⁵ “MSF Calls for No Patents or Profiteering on COVID-19 Drugs, Tests, and Vaccines in Pandemic.” *Médecins Sans Frontières Access Campaign*, Doctors Without Borders, 27 Mar. 2020, <https://msfaccess.org/msf-calls-no-patents-or-profiteering-covid-19-drugs-tests-and-vaccines-pandemic>; Varoon Mathur. “Will Bayh-Dole Be Needed to Get Affordable Covid-19 Treatments?” *STAT*, 1 Apr. 2020, www.statnews.com/2020/04/02/invoking-bayh-dole-may-be-needed-to-get-affordable-covid-19-treatments/;

⁶⁶ Joseph A. DiMasi, et al. “Innovation in the Pharmaceutical Industry: New Estimates of R&D Costs.” *Journal of Health Economics*, North-Holland, 12 Feb. 2016, www.sciencedirect.com/science/article/abs/pii/S0167629616000291?via=ihub.

regulatory burden of bringing a drug to market.⁶⁷ For its part, the RSC has promoted utilizing EUREKA prize competitions, existent law which would award private industry on a results-oriented basis.⁶⁸

Outlook

Few would argue that an effective public health response to the COVID-19 pandemic must successfully coordinate broad access to testing, well-informed mechanisms to track those infected, and accelerated pathways to producing effective treatments for the disease. These issues are not mutually exclusive. As the House E&C report notes, testing and contact tracing are both key parts of a wider COVID-19 surveillance system. Taken together, these issues will bring to the fore varied constitutional, practical, and economic considerations conservatives will need to consider. Further, attempts by the Left to gain more footholds into private industry will come in varied forms. As America contends with its gravest economic crisis since the depression, the attempts are likely to grow bolder and more pronounced. Conservatives would be wise to advance targeted, timely, and evidence-based reforms as another potential recovery package looms.

⁶⁷ Fred Reinhart. "Using Bayh-Dole March-in Rights Would Slow Covid-19 Innovation." *STAT*, 1 May 2020, www.statnews.com/2020/05/04/bayh-dole-march-in-rights-handicap-covid-19-innovation/.

⁶⁸ "Johnson, Marshall Unveil Proposal to Unleash Health Care System in Fight Against COVID-19." *Republican Study Committee*, 27 Apr. 2020, <https://rsc-johnson.house.gov/news/press-releases/johnson-marshall-unveil-proposal-unleash-health-care-system-fight-against-covid>.



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES **Office for Civil Rights**

Guidance on HIPAA and Contacting Former COVID-19 Patients about Blood and Plasma Donation

Does HIPAA permit a covered health care provider to use protected health information (PHI) to identify and contact patients who have recovered from COVID-19 to provide them with information about donating blood and plasma that could help other COVID-19 patients?

Yes. Generally, a covered health care provider may use PHI to identify patients who have recovered from COVID-19 to provide them with information about how they can donate their blood and plasma containing antibodies to the virus that causes COVID-19, to help treat other patients with COVID-19.¹

The HIPAA Privacy Rule permits HIPAA covered entities (or their business associates on the covered entities' behalf) to use or disclose PHI for treatment, payment, and health care operations, among other purposes, without an individual's authorization.² Health care operations include population-based activities relating to improving health, and case management and care coordination activities that do not meet the definition of treatment (*e.g.*, where such activities are not connected to the care of a specific patient).³ When using or disclosing PHI for health care operations, the covered entity must make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.⁴

The use of PHI to identify and contact patients who have recovered from COVID-19 for this purpose is permitted as a population-based health care operations activity of the covered health care provider because facilitating the supply of donated blood and plasma would be expected to improve the

¹ Plasma collected from individuals who have recovered from an infection is called "convalescent plasma." The Food and Drug Administration (FDA) has issued guidance to provide recommendations to health care providers and investigators on the administration and study of investigational convalescent plasma collected from individuals who have recovered from COVID-19 (COVID-19 convalescent plasma) during the public health emergency, available at <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/investigational-covid-19-convalescent-plasma>.

² See 45 CFR 164.502(a)(1)(ii) and 164.506.

³ See 45 CFR 164.501 (defining "health care operations," and "treatment"). Additional discussion of the difference between treatment and health care operations under the HIPAA Privacy Rule can be found in the 2000 Final Privacy Rule at 65 FR 82462, 82626 (December 28, 2000).

⁴ See 45 CFR 164.502(b) and 164.514(d).

provider's ability to conduct case management for patient populations that have or may become infected with COVID-19.⁵

A covered health care provider may identify and contact its patients for this purpose, without authorization, to the extent that this activity does not constitute marketing. Marketing is a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service.⁶ Generally, the HIPAA Privacy Rule prohibits the use or disclosure of PHI for marketing purposes without a patient's authorization.⁷ Thus, communications that inform or encourage patients who have recovered from COVID-19 regarding the means and benefits of donating blood and plasma and encourage such patients to use any particular blood and plasma center(s) for such donations would constitute marketing, unless the communication meets an exception to the definition of marketing. Under one exception to the definition, a covered health care provider is permitted to make such communication for the covered entity's population-based case management and related health care operations activities,⁸ provided that the covered entity receives no direct or indirect payment from, or on behalf of, the third party whose service is being described in the communication (*e.g.*, a blood and plasma donation center).⁹

While the HIPAA Privacy Rule permits a covered entity to use PHI to identify and contact its own former COVID-19 patients, a covered entity generally cannot disclose PHI to a third party, without the individuals' authorization, for the third party to make marketing communications about the third party's products or services, unless the third party is making the communication on behalf of the covered entity (*i.e.*, as a business associate). For example, a hospital cannot disclose PHI about individuals who have recovered from COVID-19 to a blood and plasma donation center, so that the donation center can contact the patients to request blood and plasma donations for its own purposes.¹⁰ In such cases, the covered entity would need to obtain the individuals' authorization prior to making such a disclosure.

⁵ See 45 CFR 164.501 (definition of "health care operations" (1): "Conducting . . . population-based activities relating to . . . case management . . .").

⁶ See 45 CFR 164.501 (definition of "marketing," ¶ 1).

⁷ *Id.*

⁸ See 45 CFR 164.501 (definition of "marketing," ¶ (2)(ii)(C)).

⁹ See 45 CFR 164.501 (definition of "marketing," ¶¶ (2)(ii)(C), (3)).

¹⁰ A disclosure to the blood and plasma center, for the blood and plasma center's own purposes, is not considered to be for the health care operations of a hospital as a covered entity. However, a hospital may disclose PHI about individuals who have recovered from COVID-19 to a blood and plasma donation center that is working with the hospital to improve the hospital's ability to conduct case management for patient populations that have or may become infected with COVID-19, if the hospital enters into a business associate agreement with the blood and plasma donation center.

Privacy and Security Round Up

Bipartisan Contact Tracing Privacy Bill Introduced in Congress

On June 1, 2020, Senators Cantwell (D-WA), Cassidy (R-LA), and Klobuchar (D-MN) introduced the first bipartisan contact tracing privacy bill. The bill, the Exposure Notification Privacy Act, applies to data that is linked or reasonably linkable to an individual or to the individual's device and that is collected or processed in connection with an "automated exposure notification service" ("AENS"). An AENS is any website, application or online service specifically designed or marketed for the purpose of automatically notifying an individual exposed to an infectious disease. The bill allows the operation of an AENS only in collaboration with a public health authority, and requires the individual's affirmative express consent to enroll in the AENS. It prohibits use of the data for a commercial purpose, and allows data to be transferred to a service provider for only limited purposes. However, it does not prohibit the use of the data for human subject research, including public health research. Like the previously introduced Republican and Democratic bills on contact tracing privacy, it requires the provision of a privacy notice, data minimization, data deletion when no longer needed for the purpose collected, and security measures (including, in this bill, security breach notification requirements). While the bill provides for enforcement by the Federal Trade Commission (FTC) and State Attorneys General, it also explicitly preserves state laws, including state common law and causes of action for civil relief.

Comments: While the bipartisan bill is more limited in scope than the other two bills in terms of the entities it would likely reach, it is also arguably the most restrictive and, unlike the other two bills, it is not limited to the COVID-19 public health emergency or COVID-19 related data. It is yet to be seen whether any of these bills will gain traction.

Facial Recognition Software Under Scrutiny Again

On June 10, 2020, Amazon announced that it was putting in place a one-year moratorium on the use of its facial recognition software by law enforcement in order to give government the opportunity to "put in place stronger regulations to govern the ethical use of facial recognition technology." This statement was echoed by Microsoft later on the same day, when it announced that it would not sell its facial recognition software to law enforcement until there is a "national law, grounded in human rights" governing its use. Both statements came in the wake of a June 8, 2020 announcement by IBM that it was exiting the facial recognition business, and follow the announcement by the ACLU on May 28, 2020, that it had filed a lawsuit against Clearview AI, claiming that its facial recognition technology violated the Illinois Biometric Privacy Act. Then, on June 11, 2020, the European Data Protection Board stated that the use of Clearview AI's facial recognition product by law enforcement would "likely not be consistent with the EU data protection regime."

Comments: Amazon and Microsoft appear to have come round to Google's view, when it stated in January 2020 that it supported a temporary moratorium on the use of facial recognition software to give government a chance to "chart the course", following reports that the EU was considering such a moratorium. However, even as these tech giants are embracing a national framework and regulation for the use of facial recognition software, some in the public are now calling for banning its use entirely, at least by law enforcement. As with contact-tracing technology, a middle ground will need to be reached that balances the benefits of this new technology against the risks of its misuse.

CCPA Regulations Await Approval to Become Final

On June 1, 2020, the California Attorney General (AG) submitted the text of the final California Consumer Protection Act (CCPA) proposed regulations, along with the Final Statement of Reasons, to the California Office of Administrative Law (OAL) for review under the California Administrative Procedure Act. The California AG also posted these documents on its website. The text of the proposed final regulations is unchanged from the proposed regulations issued on March 11, 2020. The OAL has 30 working days plus an additional 60 calendar days pursuant to an Executive Order related to the

COVID-19 pandemic to perform this review. However, the California AG has requested that the OAL expedite its review so that the final regulations can be effective on July 1, 2020, the date the California AG is authorized to begin enforcement of the CCPA.

Comments: The Final Statement of Reasons, particularly the Appendices summarizing the California AG's response to comments, provides some useful additional guidance to assist in interpreting the CCPA requirements. However, it is notable that in response to a number of comments the California AG stated that it was not addressing the issues raised in order to prioritize "the immediate implementation of the law." Hopefully this means that the California AG intends to issue guidance on these issues once the regulations are finalized.

OCR Issues Guidance on Contacting Former COVID-19 Patients About Blood and Plasma Donations

On June 12, 2020, the HHS Office of Civil Rights (OCR) issued [guidance](#) explaining that health care providers may use protected health information (PHI) to identify patients who have recovered from COVID-19 to tell them about donating their blood and plasma to help treat other patients with COVID-19. OCR states that this use of PHI is a permitted population-based health care operations activity of the covered health care provider because it is expected to improve the provider's ability to conduct case management for patient populations that have or may become infected with COVID-19. OCR cautions that in order to be able to be able to make these communications without patient authorizations, the providers must ensure that communications do not constitute marketing. OCR then goes on to explain that these types of communications should fall within a marketing exception as long as the provider does not receive any direct or indirect payment from the donation center for making the communication. Finally, OCR makes clear that while a provider may disclose the PHI to a business associate to make the communications on its behalf, it may not provide the PHI to third parties not acting on its behalf, such as to donation centers acting on their own behalf, to contact the patients directly.

Comments: The OCR guidance is helpful in providing assurance to covered health care providers that OCR regards this use of PHI as a permitted population-based health care operation purpose, even though there is apparently no necessary connection, contractual or otherwise, between donation center and provider.

Google Faces Class Action Lawsuit for Tracking Users, Even Those Using Private or Incognito Browsing Mode

On June 2, 2020, a class action [lawsuit](#) was filed against Google in the U.S. District Court of Northern California seeking damages of at least \$5000 per person for violations of the Federal Wiretap Act and California Invasion of Privacy Act. The complaint claims that Google tracks and collects data of users even when they choose to browse in "private browsing" mode. According to the complaint, Google used Google Analytics, Google Ad Manager, and various other application and website plug-ins to collect consumer browsing history and other web activity data "no matter what safeguards consumers undertake to protect their data privacy." This lawsuit follows a [lawsuit](#) filed on May 27, 2020 by the Arizona Attorney General against Google for violations of the Arizona Consumer Fraud Act by deceptively collecting location data of users, even when the users thought they had disabled location data collection.

Comments: Both lawsuits focus on Google's allegedly deceptive conduct and, in the case of the California lawsuit, makes the rather novel argument that Google's conduct violates the Federal Wiretap Act by intentionally intercepting internet communications. This argument is likely made because the Federal Wiretap Act provides a private right of action, and so highlights the fact that there is not yet a comprehensive national privacy law governing data collected from individuals and/or the devices that would allow such individual recourse for its misuse.

Please contact Diane Sacks at dsacks@sacksllc.com or (202)459-2101 for more information on any of these items. This newsletter is intended to provide general information only and is not intended as legal advice.



CORONAVIRUS

Getting it right: States struggle with contact tracing push

Digital tools for tracking Covid-19 could prove less useful if there are major gaps in data.



A nurse administers a coronavirus test. | Ted S. Warren/AP Photo

By **ALICE MIRANDA OLLSTEIN** and **MOHANA RAVINDRANATH**

05/17/2020 07:00 AM EDT



A half-dozen states have announced they're building their own apps to pinpoint the spread of coronavirus so they won't have to rely on similar efforts from distrusted big tech firms. So far, it's not going well.

North Dakota is getting spotty data from cell phone towers after relying on an app originally designed to connect its state university football fans on road trips to away games. Utah delayed the rollout of a GPS tracking function after technical difficulties. Other states, like Georgia, are promoting tools that rely on people to self-report new Covid-19 infections, potentially creating gaps in the effort to track the spread of the virus.

Advertisement

AD

Most states are waiting to see whether the Bluetooth-based release from Apple and Google, which is supposed to automatically notify people when they come close to someone who's tested positive, will be an effective way to monitor outbreaks. Some states are raising concerns that the tech giants' app won't allow them to collect enough information due to privacy concerns.


But the new state apps may still be viewed skeptically by a public reluctant to submit to digital tracking. And the early experience of these states is raising questions about whether locally developed apps will gain enough critical mass to help health officials keep tabs on the virus before new hot spots explode. At least one state, North Dakota, is now embracing the Apple-Google collaboration.

Regardless of states' differing approaches to digital contact tracing, public health experts agree they face a high hurdle getting enough people to trust virtual surveillance to make the effort worthwhile. Almost 60 percent of Americans said they couldn't or wouldn't use the system Apple and Google are developing, according to a [recent Washington Post-University of Maryland poll](#).

CORONAVIRUS: WHAT YOU NEED TO KNOW

As deaths mount, **many nursing home facilities are not being checked** for proper procedures.

Confirmed U.S. Cases: **2,115,079** | U.S. Deaths: **116,191**

 **How coronavirus will change the world permanently**

 **Coronavirus cases, tracked state by state**

 **Do you work for a hospital?** Tell us what you're seeing

TOP DEVELOPMENTS

- A cheap steroid is the first to **reduce deaths in coronavirus patients**, British researchers found.
- Florida Gov. Ron DeSantis wants to shift the focus **from the pandemic to economic recovery**.
- The **kill-switch effect** of the shutdown is immediately evident in cities, where many businesses have closed for good.
- **The father of Minnesota Rep. Ilhan Omar** has died of coronavirus.

[Read all coronavirus coverage »](#)

“Either you have a system unlikely to help people navigate their world, to leave their house and feel safe, or you have privacy trade-offs.” said University of Washington Law School professor Ryan Calo, who recently co-authored [a study that found widespread public discomfort with contact tracing technology](#).

The North Dakota app relies on nearby cell towers and Wi-Fi to follow users’ GPS locations. The state says the technology protects privacy by assigning users a random ID number for tracking movements, and it does not collect personally identifiable information.

Vern Dosch, who heads North Dakota’s contact tracing efforts, said officials believed this approach was better suited for the sparsely populated state — but location data has turned out to be spotty, given that over 20 percent of the population doesn’t have broadband at home. [Some app users have complained it often failed](#) to log where they spent time or placed them in locations they never visited.

Fewer than 34,000 North Dakotans have signed up so far, below the state’s original goal of 50,000 — and well short of the 100,000 that Dosch said would provide the state with a much fuller picture. Dosch’s team is working on a marketing campaign aimed at boosting enrollment and addressing residents’ privacy concerns.

In a reversal, residents later this month will have the choice of using a new version of the app incorporating Google’s Bluetooth technology. Dosch acknowledged the state’s decision to partner with the company might worry some, but he said it’s more important to have accurate data on the virus.

"While there’s no question we’ve gotten people who have voiced concerns, and there’s always conspiracy theories out there, in the end it’s about risk and reward," Dosch said. "We want to fall on the side of giving our citizens every protection we can give them, and if that involves aligning with Apple and Google, then that’s what we’re going to do."



HEALTH AFFAIRS BLOG

RELATED TOPICS:

COVID-19 | PRIVACY

| HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

| TECHNOLOGY | REGULATION | PUBLIC HEALTH

Protecting Privacy In Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork

Carmel Shachar

MAY 19, 2020 10.1377/hblog20200515.190582



Contact tracing for COVID-19 is a necessary tool to allow communities to reopen. Unfortunately, because of the speed and numbers of COVID-19 cases, manual contact tracing is unlikely to be sufficient. [Digital contact tracing can provide enough capacity](#) but comes with serious



Get Our Newsletters

First Name

Last Name

Email*

Sign Up Today

Related

CONTENT



privacy concerns.

Digital contact tracing substitutes mobile apps for individuals who track down instances of COVID-19 exposure through interviews with coronavirus carriers. Individuals install these applications on their phones. The app uses either GPS or Bluetooth data to record when two users have been in close proximity of each other for a sufficiently long period of time for the virus to be transmitted. When a user reports that he or she is COVID-19 positive, the application can immediately alert other users who were near the infected user, encouraging them to get tested.

In the United States, digital contact tracing falls into a strange category in which at times it is governed by the Health Insurance Portability and Accountability Act (HIPAA), but at times not. There are efforts, led by the Senate, to implement data privacy regulations to more broadly cover digital contact tracing. Unfortunately, these efforts would create an unworkable regulatory patchwork in conjunction with HIPAA. We should rethink our approach to the governance of digital contact tracing data to create one regulatory regimen to oversee these programs and maximize consumer protections, regardless of who is implementing the apps.

The Need For Contact Tracing And Contact Tracing Privacy Regulations

Contact tracing apps are an increasingly popular tool to combat COVID-19. Most are [structured similarly](#). For example, Jane Smith downloads an app that records when she is in proximity to any other phone with the tracing app. If she tests positive for COVID-19, Jane uploads this information to the contact tracing app, which in turn sends that information to all the other phones that were close enough during the key incubation period. The users of these phones receive a notification that they were exposed to COVID-19 and are urged to get tested. However, they are

COVID-19

TOPICS



COVID-19

Privacy

Health

Insurance

Portability And
Accountability
Act Of 1996

Technology

Regulation

Public Health

Cite As

"Protecting Privacy In Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork," Health Affairs Blog, May 19, 2020.

DOI:

10.1377/hblog20200515.190582

not told that Jane tested positive or even when they were exposed. Public health departments may be notified by the app, but not always. The app could be structured to require a health care worker to upload testing outcomes, but that is not a necessary feature.

In this sense, digital contact tracing differs from manual contact tracing. Manual contact tracing takes advantage of the “human touch” because professional contact tracers can connect sick individuals to social and medical supports. The human element is also a drawback of manual contact tracing because it relies on an infected individual to remember who they were near and provide contact information for them. Digital contact tracing does not suffer from this memory problem. It is also extremely scalable and fast to implement because local authorities do not have to spend time and resources training people as contact tracers.

Singapore, with its [TraceTogether](#) app, was an early pioneer of digital contact tracing. Many other countries including [Australia](#), [Germany](#), and the [United Kingdom](#) are working to rapidly implement these apps. In virtually all countries, including the United States, the use of these apps is voluntary. For contact tracing apps to be effective, however, [approximately half of the country’s total population](#) must become users. We are talking about a treasure trove of data, including personal health information and location.

In the United States, Google and Apple recently announced the [details of a contact tracing app](#) they are jointly developing. To minimize privacy concerns, the two technology companies have focused on Bluetooth-based proximity detection and designed the app to hold most information on users’ phones rather than servers. Because neither Google nor Apple meet the definition of a [covered entity under HIPAA](#), the law’s privacy enforcing requirements do not apply to the companies’ contact tracing efforts. In some states, such as California, state

laws may provide some protections, but not every state has applicable laws or regulations. The lack of privacy regulations mean that users will have to depend on the good will of technology companies to avoid misusing data or violating their privacy. On April 10, 2020, in a [letter to Jared Kushner](#), Senators Mark Warner (D-VA) and Richard Blumenthal (D-CT), along with Representative Anna Eshoo (D-CA), recognized this problem, asking “[w]hat measures will the Administration put into place to ensure that the public health surveillance initiative protects against misuse of sensitive information?”

New Proposal To Cover Some Contact Tracing Efforts

The answer seemed to appear on April 30, 2020. Several Republican Senators, including Senate Commerce Committee Chairman Roger Wick (R-MS), Majority Whip John Thune (R-SD), and Senators Jerry Moran (R-KS) and Marsha Blackburn (R-TN) [announced](#) plans to introduce the COVID-19 Consumer Data Protection Act. This act would govern contact-tracing apps operated by organizations not subject to HIPAA. Companies would have to be transparent about their data collection and usage and obtain individuals’ express consent before collecting, processing, or transferring data collected by these apps. Individuals would also have the right to opt-out of data collection. Additionally, companies would need to de-identify all personally identifiable information when it is no longer being used for the health emergency. Enforcement of this act would rest with the Federal Trade Commission (FTC) and state attorney generals.

The proposed bill addresses a clear need for the regulation of contact-tracing apps. Unfortunately, it does not harmonize well with our existing data governance and privacy regimens. In many ways the act is similar to newer generation privacy regimens such as the European Union’s [General Data Protection Regulation](#) (GDPR) and the [California Consumer Privacy Act](#) (CCPA) when it comes to

consent, transparency, data deletion, data minimization, and security. For example, the act, GDPR, and CCPA all allow individuals to compel their data to be deleted upon an opt-out request.

The act's approach to data privacy and governance puts it at odds with HIPAA, in that the act provides more protections for users in some respects and fewer protections in other key regards. For example, unlike the act, HIPAA does not provide individuals a "right to be forgotten;" that is, to be deleted upon request from a data set or require affirmative consent before the medical provider can enter an individual's data into a database. On the other hand, the act would allow covered entities to use consumer geolocation or personal health information for purposes beyond COVID-19 contact tracing, including selling data or using it for marketing purposes. This is in stark contrast to HIPAA, which allows covered entities to sell protected health information only if they have obtained authorization from all individuals whose identifiable health information is included in a patient data set compiled by the covered entity. This is especially worrisome because users may assume that HIPAA protections apply to contact tracing apps and provide information they would not want sold or used for marketing.

The Need For An Overarching Regulatory Regimen For Contact Tracing

While HIPAA was written before the mobile app and smartphone revolution, it is important to consider how any legislation governing the use of information to combat COVID-19 would interact with it. It seems strange that Google or Apple would have different data requirements than a hospital operating a contact-tracing app, when the privacy impact on users would be the same no matter the creator. This also raises questions of which privacy regimen to follow in the case of a collaboration between a HIPAA covered entity and an entity that would be covered under this act. If a hospital contributed COVID-19

diagnoses or test results to a contact-tracing app that also used geolocation data and was operated by a non-HIPAA covered entity, we may see a database that had a patchwork of requirements relating to consent, right to be forgotten, and allowable uses. Furthermore, giving enforcement power to the FTC rather than to the Department of Health and Human Services (which customarily pursues HIPAA violations) may make it more difficult to address health data privacy violations.

The act is a good acknowledgment that we need governance of contact-tracing apps, both because they are likely to be widely used until there is a vaccine and because they pose serious privacy concerns. But it does not correctly harmonize with existing privacy regulations. Contact-tracing apps are public health and quasi-medical by nature. A successful regulatory regimen would not merely try to address what is not currently protected by HIPAA. A more regulatorily consistent approach would be to extend at least the most relevant HIPAA obligations to these apps, which would prevent companies from selling or using data for marketing purposes. An even better approach might be to impose the same regulatory regimen on all digital surveillance and contact-tracing efforts, including those operated by HIPAA covered entities. In that way, we can think of HIPAA as the “floor” and the newer regulations as privacy maximizing requirements. Either way, we would avoid creating silos of data based on the creator and implementor of the contact tracing app.



This website uses a variety of cookies, which you consent to if you continue to use this site. You can read our **privacy policy** (<http://www.xtelligentmedia.com/privacy-policy>) for details about how these cookies are used, and to grant or withdraw your consent for certain types of cookies. Consent and dismiss this banner by clicking agree.

Agree



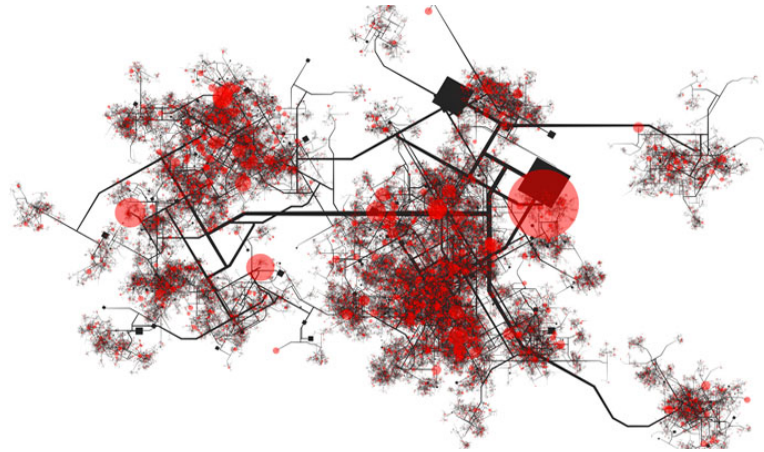
Search... login | register

- Home (<https://healthsecurity.com/>)
- News (<https://healthsecurity.com/news>)
- Features (<https://healthsecurity.com/features>)
- Interviews (<https://healthsecurity.com/healthcare-information-security-interviews>)
- Podcasts (<https://www.xtelligentmedia.com/podcasts>)
- Mobile (<https://healthsecurity.com/topic/healthcare-mobile-security>)
- Data Research (<https://www.xtelligentmedia.com/insights>)
- White Papers & Webcasts (<https://healthsecurity.com/resources/topic/it-security>)

PATIENT PRIVACY NEWS

COVID-19 Contact Tracing Apps Spotlight Privacy, Security Rights

As tech giants like Microsoft, Google, and Apple move to craft the APIs behind COVID-19 contact tracing apps, privacy advocates rush to ensure the protection of privacy and cybersecurity rights.



<https://www.facebook.com/share.php?u=https%3A%2Fhealthsecurity.com%2Fnews%2F%2Fcovid-19-contact-tracing-apps-spotlight-privacy-security-rights&title=COVID-19%20Contact%20Tracing%20Apps%20Spotlight%20Privacy%20Security%20Rights>  (<https://twitter.com/intent/tweet?text=COVID-19%20Contact%20Tracing%20Apps%20Spotlight%20Privacy>)

%2C%20Security%20Rights&url=https%3A%2F%2Fhealthitsecurity.com%2Fnews%2Fcovid-19-contact-tracing-apps-spotlight-privacy-security-rights) 
https://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fhealthitsecurity.com%2Fnews%2Fcovid-19-contact-tracing-apps-spotlight-privacy-security-rights&title=COVID-19%20Contact%20Tracing%20Apps%20Spotlight%20Privacy%20Security%20Rights)



By Jessica Davis (mailto:jdavis@xtelligentmedia.com)

May 20, 2020 - Contact tracing app initiatives have emerged in the wake of the COVID-19 pandemic, as a modern enhancement to traditional methods for tracking the spread of the virus, finding new infections, and supporting the reopening of the economy.

Several tech giants and public health authorities across the globe have quickly signed on to build the application programming interfaces (APIs) and apps necessary to support the scale of the project. In the US, some states have implemented their own versions, while Microsoft has partnered with the University of **Washington** (<https://www.washington.edu/news/2020/04/22/a-contact-tracing-app-that-helps-public-health-agencies-and-doesnt-compromise-your-privacy/>) on a new app designed to help public health agencies.

But the rare partnership between Google and **Apple** (<https://healthitsecurity.com/news/sens.-probe-privacy-cybersecurity-of-apple-covid-19-screening-tools>) has generated the most interest, given the companies' past privacy concerns and the planned use of Bluetooth Low Energy technology to inform individuals when they've been exposed to someone who has COVID-19.

The American Civil Liberties **Union** (<https://healthitsecurity.com/news/aclu-scientists-urge-privacy-focus-for-covid-19-tracing-technology>), a group of 200 scientists, and the Electronic Frontier **Foundation** (<https://healthitsecurity.com/news/eff-warns-covid-19-tracing-apps-pose-cybersecurity-privacy-risks>) have all released reports outlining potential privacy and cybersecurity risks developers should consider when both building the API and drafting privacy policies.

For the ACLU, the concern lies with potential overreach, discrimination, and ensuring participation is voluntary. The groups are also concern the developers have not created an exit strategy for sunseting the data generated during the pandemic after it has ended.

READ MORE: Apple, Google Address COVID-19 Contact Tracing App Privacy Concerns (<https://healthitsecurity.com/news/apple-google-address-covid-19-contact-tracing-app-privacy-concerns>)

Google and Apple have responded to those concerns with a transparent list outlining its **practices** (<https://healthitsecurity.com/news/apple-google-address-covid-19-contact-tracing-app-privacy-concerns>), as well as its plans to disable the service at the end of the pandemic.

Despite those assurances, a study by the Washington **Post** (<https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-to-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/>) and the University of Maryland revealed that three in five Americans would be either unwilling or unable to use the contact tracing system. The trouble is that the success of these apps rest on user participation.

Which begs the question: Can these privacy and security risks be overcome to assure individuals their data will only be used in the fight against the spread of COVID-19?

As Google and Apple released their API on **May 20** (<https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/>) and privacy concerns remain prominent, *HealthITSecurity.com* spoke with a range of privacy and security leaders to dive deeper into some of these concerns and the functions developers must consider to restore individuals' trust in these technologies.

"The COVID-19 pandemic is presenting novel privacy and security challenges as public health authorities navigate the prospect of widespread contact tracing initiatives," said Sherrese Smith, vice-chair of Paul Hastings' Data Privacy and Cybersecurity practice. "Privacy laws and regulations continue to change, as do consumer expectations on the use of data by both public and private entities."

READ MORE: EFF Warns COVID-19 Tracing Apps Pose Cybersecurity, Privacy Risks
(<https://healthitsecurity.com/news/eff-warns-covid-19-tracing-apps-pose-cybersecurity-privacy-risks>)

"How the COVID-19 response evolves will have significant impacts on how data protection laws are crafted and implemented in the future," she continued. "This is particularly true in the United States, which has yet to adopt a national privacy protection law and could see significant legal changes in the next few years."

THE CRUX OF PRIVACY CONCERNS

Contact tracing apps are integral to tracking and stopping the spread of COVID-19, and those willing to turn over their personal information to "do their part" to address the virus have some level of expectation for a reduction in their personal privacy to do so, explained attorney Jena Valdetero, a partner of Bryan Cave Leighton Paisner.

"Bluetooth was not designed for contact-tracing, so it is a somewhat blunt tool for identifying potential COVID-19 exposure."

However, it is crucial people have an understanding of what they're giving up in exchange for participation and its benefits.

For Valdetero, those risks are tied to apps that allow you to identify particular users through the app's reliance on GPS to track people's movements, or due to users living in sparsely populated geographic areas that make it "difficult to truly anonymize the data."

READ MORE: Congressional Bills Target COVID-19 Contact Tracing App Privacy
(<https://healthitsecurity.com/news/congressional-bills-target-covid-19-contact-tracing-app-privacy>)

Many of the proposed apps will rely on geo-location tracking, but this poses another issue with whether individuals understand the extent to which they're giving the app an "almost uncomfortable degree of insight into their daily activities."

"While there is a clear public health need and individual benefit to people to participate in contact tracing, most people are uneasy about the idea that the government – or a hacker – may be able to tell exactly where they go and when," Valdetero said.

"The prevailing view seems to be that Bluetooth technology will address the concern that the apps will be able to identify the users individually, which is true, and is particularly important if the information is going to be shared with the government," she added.

As a result, anyone with whom the user comes in contact may be able to determine who was exposed based on their own interactions. And Valdetero is unsure how app developers could address that risk.

These concerns were also shared by Smith, as even Bluetooth-based proximity tracing could lead to the discovery of a person's infection status. Those with a limited number of physical contacts could easily use their own device contact log to identify the family and friends who self-reported positive infection statuses through contact-tracing apps.

To Smith, the risks are also tied to over inclusive results and increased surveillance.

“Many advocates are also concerned about the risk of false-positives and knock-on effects for individuals that have been notified of involuntary exposure,” she said. “Bluetooth was not designed for contact-tracing, so it is a somewhat blunt tool for identifying potential COVID-19 exposure.”

“Proximity is only one factor in virus exposure and may be less significant than other factors, such as wearing a face mask,” she added. “Relying solely on proximity risks creating a database that overestimates potential exposure events. If a ‘clean’ proximity record becomes necessary for some individuals to go back to work or get life insurance, over-inclusion can result in real-world negative consequences.”

Further, data needs to be collected at scale for these contact tracing apps to be effective, Smith stated. So the concern of many, and perhaps rightly so, is that these systems designed to contain COVID-19 will end up serving as the basis for more widespread digital surveillance in the future.

Heather Federman, vice president of privacy and policy at BIGID, a data privacy firm took it a step further, explaining concerns around data retention and secondary use are valid. After 9/11, FISMA took on a wide sweep of data through a consumer facing application, which was later found to be used for other purposes. The data was also meant to be sunsetted after a specific period of time, but provisions are still in place to allow the data collection to continue.

“Every disclosure of personal information comes with some latent risk that it will be used in the future for purposes not disclosed at collection.”

Right now, **Congress (<https://healthitsecurity.com/news/congressional-bills-target-covid-19-contact-tracing-app-privacy>)** is considering competing legislation designed to shore up some of these issues and ensure collection ends after the pandemic, but Federman mused: “How do we know that it’s actually going to happen?”

“It goes to a greater point that a lot of advocates have made that these apps could open a door to do more surveillance,” Federman said. “Right now, apps are being developed specifically around COVID-19, but who’s to say it wouldn’t be used to determine who’s vaccinated or for performing a general health check.”

“We have to be sure that these apps will not be used by governments for increased unwarranted public surveillance,” Kelvin Coleman, executive director, National Cybersecurity Alliance (NCSA). “Although it’s still in its early days, and we haven’t seen anything conclusive here, it’s something people should be thinking about moving into the post-COVID-19 world.”

Coleman added that these apps are “also a double-edged sword” when it comes to privacy. The apps will be instrumental for notifying people of potential exposures, but they’ll be sharing more private information on those reentering society. Concerns shared by advocates are valid, as data breaches will be more likely with mass data collection and centralized storage.

The apps could also exacerbate potential threat vectors, through phishing scams, ransomware, and the like, he explained.

“There are warnings about the risks that have already had some impact and have helped Google and Apple limit and constrain their approach,” said Tom Pendergast, MediaPRO’s chief learning officer. “But the risks are just huge in terms of collecting really sensitive personal information.”

“Who has access to it? And how do we put limitations on what can be done with it? And how do we sunset the data? And if we start to identify certain people as infected, the data will be more susceptible to ending up into the wrong hands or government overreach. Those individuals could be stripped of basic, and even human rights,” he added. “I don’t think privacy risks get any more fundamental than that.”

If the information ends up in the wrong hands or used in an inappropriate way, people could be stripped of their rights, stressed Pendergast.

Smith added: “Balancing urgent public health needs and the slow erosion of privacy rights over the long term is an important public policy issue that is being prompted by these unprecedented times.”

THE POTENTIAL FOR OVERREACH

One of the biggest concerns brought to light by the ACLU insights is the potential for

overreach. And while Congress is working to craft privacy legislation for COVID-19 contact tracing, Federman explained that it's highly unlikely legislators will come to a compromise ahead of the release of these apps.

The lack of a comprehensive privacy law has only fueled concern around the use of these apps, explained Coleman. The other concern lies with just what information can be accessed and to which organization.

"App developers should work with privacy counsel to develop clear consent mechanisms, plain-language privacy notices, and easy-to-use opt-out procedures."

Those surveillance concerns have stemmed from instances in the UK and India, where Coleman said its citizens have experienced unprecedented watchdog scrutiny. While the US has broader freedoms, without a federal privacy law, "transparency could be up to developers' discretion. Whether the pendulum swings in favor of the people's privacy will remain to be seen."

"The problem is that it's hard to control overreach," Federman said. "It comes down to accepting that you can't always control for everything, but we do our best to try and control the system and ensure the initial setup has all of these privacy controls in place, especially around secondary data use."

"But it must also come with an internal audit and risk assessment into how the tech is using data, and whether they're using it on a personal level," she continued. "Some aggregate data could be useful... but if they're using data for any additional purpose beyond contact tracing, stakeholders must have users' rights in place through an ethical review."

The key will be a mixture of external transparency, as well as contractual controls in the agreements between developers and third-party apps. Valdetero noted that the third-party apps could be tempted to use the data collected by contact tracing apps for other purposes not contemplated at the time the information was collected.

As a result, developers must draft and provide users will clear and comprehensive privacy policies that outline the precise data they'll collect, how it's used, and to whom the data will be shared, Valdetero said.

The policy will need to clearly state the data will only be used for the purpose of contact tracing and addressing the pandemic and not for other purposes, she explained. And if the intent of the use of data changes during that time, such as researchers learning the data could help with COVID-19 in another way, then those developers must first get opt-in permission from users before they do so.

"Every disclosure of personal information comes with some latent risk that it will be used in the future for purposes not disclosed at collection. Location data that could potentially be linked to individual users can be quite valuable," Smith said. "This is why it is critical for developers to minimize data collections and build in privacy by design wherever possible."

"With privacy, an ounce of prevention is better than a pound of cure," she added. "So before signing up for these apps, users should take the time to understand the data that is collected, applicable privacy policies, and the app provider's reputation. Privacy protection is a competitive advantage these days and enforcement of privacy laws is widespread, so companies take significant risks when they use data for novel purposes."

INHERENT CYBERSECURITY RISKS

Several proposed contact tracing apps will rely heavily on Bluetooth technology for tracking individuals and potential exposures. While Smith stressed that any contact tracing system will come with its own inherent security risks, Bluetooth-based platforms will have inherent vulnerabilities to correlation attacks.

In these exploits, hackers leverage external data, like photos, video, or facial recognition templates to identify anonymized data.

"For example, it is conceivable that a bad actor could install a video camera outside of a health clinic and later pair the video with data from the contact tracing app to link anonymized keys to individual faces," Smith said.

"While certainly possible at the local level, it does seem somewhat unlikely that such correlation attacks would be scalable by bad actors," she added. "It would likely require the physical installation of video cameras and Bluetooth beacons on a large scale and may not prove attractive to hackers."

But for Smith, the critical Bluetooth vulnerability known as BlueFrag will be the biggest security challenge. Reported only in February, the flaw has still not been fixed on some Android devices. The bug could allow a remote threat actor to silently execute arbitrary code when Bluetooth is enabled.

“How the COVID-19 response evolves will have significant impacts on how data protection laws are crafted and implemented in the future.”

And with the widespread adoption of Bluetooth-based contact tracing apps, the number of Bluetooth-activated devices would also increase – as would the risk surrounding existing Bluetooth vulnerabilities, explained Smith.

There are well documented flaws in Bluetooth technology that make it an exploitable channel for attackers. In fact, the flaw is found in some medical **devices** (<https://healthsecurity.com/news/fda-warns-medical-device-bluetooth-security-flaw-could-disrupt-function>). Coleman said that as these apps plan to leverage Bluetooth tech for tracing, hackers will certainly launch cyberattacks against the tech.

KEY SECURITY REQUIREMENTS

To protect privacy and reduce cybersecurity risks, the app developers will need to implement key security requirements. Coleman explained those measures must be built upon compliance with privacy regulations.

Once compliance is established, the biggest necessity will be for developers to actively push users into ensuring they’re employing personal security measures – “especially given the dependence on Bluetooth with these apps.”

“Google and Apple have already taken a good first set of steps to better ensure privacy by barring the use of location data tracking in their contact tracing API,” Coleman said. “Other government agencies or private sector developers should ideally follow the same example.”

“They should also be transparent in communicating to users the vulnerabilities surrounding Bluetooth functionality, why enabling it on devices should be done on a needed basis, the importance of using encryption measures and enabling MFA for any apps that use or collect personally identifiable information.”

Further, with the Bluetooth flaws, users will also need to be cautious when employing the tech. And developers will need to encourage users to ensure their smartphone software is up-to-date and fully patched.

Coleman explained hackers commonly launch malicious clones that appear in app stores, which will be highly probably after the official launch of these apps. Which means that users will also need to be educated on the importance of only downloading official apps.

Valdetero added that it’s easy to “see how threat actors could lure unsuspecting users into downloading fake ones.” Users must also make sure their firmware is up to date, while developers must ensure individuals understand the importance of using the most current version of the application.

Those designing these apps should also constantly check the platforms for any vulnerabilities.

“Taking those precautions into account, Bluetooth tracing methodologies have won favor over location-based contract tracing alternatives, which would leave these tools more easily exploitable for mass surveillance uses,” Coleman said.

“Location data would allow active mapping to ID who might be meeting who, as well as when or where meetings between individuals are taking place,” he added. “Google and Apple have already ensured that governments using their joint API to develop contact tracing tools are barred from enabling location data tracking. This also mitigates the potential impacts of breaches against centralized data servers.”

Further, developers will need to monitor the contact tracing apps for vulnerabilities and issue software updates on a routine basis. Coleman stressed the need for vigilance and rapid response to overall security gaps to keep people safe at scale.

If there’s an expectation that contact tracing apps will be the key tool to reducing the spread of COVID-19, Coleman added that these measures will be critical.

Valdetero made another crucial point: “Unless the apps have the ability to cross-

communicate, the best chance of the apps meeting their stated purpose is to have everyone utilize the same app.”

“My understanding is that cross-communication functionality is part of the plan, particularly as people begin to travel between various countries and it will be important to trace traveler’s movements to identify whether and how the virus is spreading,” she added.

Ensuring the data is anonymized will also be crucial, as well as data minimization, Smith explained. Developers must commit to and ensure contact tracing apps are only collecting the necessary amount of data, as well as only sharing the minimum necessary information to help contain the spread to reduce the potential attack surface.

Fortunately, Smith explained that “any Bluetooth-based contact tracing apps have taken this to heart, using anonymized tokens and RPIDs to implement tracing and eschewing GPS-based solutions.”

In the end, cybersecurity can be maintained through developers opening up their code to scrutiny from outside groups in order to verify the security of the app, explained Pendergast. This should include auditing, pen testing, and array of security practices that will prove crucial to the development of the app.

It’s critical developers adopt the highest level of data protection practices, following the General Data Protection Regulation (GDPR) and HIPAA practices. Pendergast added that developers must be “totally transparent and above board.”

“Practically speaking, app developers should work with privacy counsel to develop clear consent mechanisms, plain-language privacy notices, and easy-to-use opt-out procedures. These are critical to ensuring transparency and fully informed consent from users,” Smith concluded.

Tagged

[Application Programming Interfaces \(https://healthitsecurity.com/tag/application-programming-interfaces\)](https://healthitsecurity.com/tag/application-programming-interfaces)

[Coronavirus \(https://healthitsecurity.com/tag/coronavirus\)](https://healthitsecurity.com/tag/coronavirus)

[Cybersecurity \(https://healthitsecurity.com/tag/cybersecurity\)](https://healthitsecurity.com/tag/cybersecurity)

[Data Privacy \(https://healthitsecurity.com/tag/data-privacy\)](https://healthitsecurity.com/tag/data-privacy)

[Interviews \(https://healthitsecurity.com/tag/interviews\)](https://healthitsecurity.com/tag/interviews)

[Patient Privacy \(https://healthitsecurity.com/tag/patient-privacy\)](https://healthitsecurity.com/tag/patient-privacy)

[f\(https://www.facebook.com/share.php?u=https%3A%2F%2Fhealthitsecurity.com%2Fnews%2F covid-19-contact-tracing-apps-spotlight-privacy-security-rights&title=COVID-19%20Contact%20Tracing%20Apps%20Spotlight](https://www.facebook.com/healthitsecurity.com/news/covid-19-contact-tracing-apps-spotlight-privacy-security-rights&title=COVID-19%20Contact%20Tracing%20Apps%20Spotlight)