Technology Policy Update
1 May 2020
By Michael Kans, Esq.

Fourth Volume of Report in 2016 Russian Hacking Endorses IC's Conclusions

In a report that largely vindicates the Intelligence Community's (IC) assessment of the 2016 election, a Senate committee continues with its investigation of Russian hacking with a heavily redacted fourth volume. The Republican-led committee rebuts the President's assertions the IC was wrong and biased.

The Senate Intelligence Committee has released the fourth of five planned volumes, detailing Russia's interference in the 2016 presidential election. This volume, titled "Review of the Intelligence Community Assessment," assessed the classified version of the Intelligence Community's (IC) review and conclusions regarding Russian efforts to aid President Donald Trump's campaign and to harm former Secretary of State Hillary Clinton's bid for the presidency. In this assessment, the Committee found "unprecedented Russian interference" well-described, analyzed, and investigated by the IC. However, much of the report is redacted, and according to Committee Member, Senator Angus King (I-ME), this was done to protect the sources and methods the IC used.

An unclassified version of "Assessing Russian Activities and Intentions in Recent US Elections" was released in mid-2017 that was heavily criticized by the President, the White House, and a number of Republicans. Additionally, the House Intelligence Committee, led by then Chair and Trump ally Devin Nunes (R-CA), found that the IC assessment was plagued by "significant intelligence tradecraft failings."

Given that the majority of Russian interference was executed in cyberspace, often through social media, it remains to be seen whether these reports will spur proposals to change laws regulating cybersecurity or U.S. intelligence activities. Moreover, like so many issues, the response to COVID-19 will likely overshadow this report and any potential impact it may have otherwise had.

While the White House has largely been silent on this volume of the Senate Intelligence Committee's investigation, the subject of Russia's activities during the 2016 election remains touchy at the White House, suggesting efforts to reform how the U.S. responds to this sort of hacking will remain at the agency-level with heads of key entities using authorities they currently possess. This opens the possibility that agencies and private sector entities will not receive new latitude to fight off disinformation campaigns likely to be waged by more than just Russia as North Korea, China, and Iran are often identified as those nations most able to interfer in this year's election.

The Committee's previous three volumes are: "Volume I: Russian Efforts Against Election Infrastructure," "Volume II: Russia's Use of Social Media," and "Volume III: U.S. Government Response to Russian Activities."

As threshold matters, the Committee found

- [S]pecific intelligence as well as open source assessments support the assessment that President Putin approved and directed aspects of this influence campaign.
- Further, a body of reporting, to include different intelligence disciplines, open source reporting on Russian leadership policy preferences, and Russian media content, showed that Moscow sought to denigrate then-candidate Clinton.
- ICA presents information from public Russian leadership commentary, Russian state media reports, and specific intelligence reporting to support the assessment that Putin and the Russian Government demonstrated a preference for candidate Trump.

The Senate Intelligence Committee made the following findings:

1. The Committee found the Intelligence Community Assessment (ICA) presents a coherent and well-constructed intelligence basis for the case of unprecedented Russian interference in the 2016 U.S. presidential election. On the analytic lines of the ICA, the Committee concludes that all [REDACTED] lines are supported with all-source intelligence, although with varying substantiation. The Committee did not discover any significant analytic tradecraft issues in the preparation or final presentation of the ICA.

The ICA reflects proper analytic tradecraft despite being tasked and completed within a compressed time frame. The compact timeframe was a contributing factor for not conducting formal analysis of competing hypotheses.

The differing confidence levels on one analytic judgment are justified and properly represented. Those in disagreement all stated that they had the opportunity to express differing points of view. The decision regarding the presentation of differing confidence levels was the responsibility of the Director of the Central Intelligence Agency (CIA) John Brennan and the Director of the National Security Agency (NSA) Admiral Michael Rogers, both of whom independently expressed to the Committee that they reached the final wording openly and with sufficient exchanges of views.

Multiple intelligence disciplines are used and identified throughout the ICA. Where the Committee noted concerns about the use of specific sources, in no case did the Committee conclude any analytic line was compromised as a result.

In all the interviews of those who drafted and prepared the ICA, the Committee heard consistently that analysts were under no politically motivated pressure to reach specific conclusions. All analysts expressed that they were free to debate, object to content, and assess confidence levels, as is normal and proper for the analytic process.

2. The Committee found that the agencies responsible for the !CA-CIA, NSA, and FBI, under the aegis of ODNI-met the primary tasking as directed by President Obama, which was to assemble a product that reflected the intelligence available to the Intelligence Community (IC) regarding Russian interference in the 2016 election.

3. The Committee found that the ICA provides a proper representation of the intelligence collected by CIA, NSA, and FBI on Russian interference in 2016, and this body of evidence supports the substance and judgments of the ICA.

[REDACTED] Regarding FBI, the ICA states, in its "Scope and Sourcing" introduction, that "[w]e also do not include information from ongoing investigations." [REDACTED] The Committee found that the information provided by Christopher Steele to FBI was not used in the body of the ICA or to support any of its analytic judgments. However, a summary of this material was included in Annex A as a compromise to FBI's insistence that the information was responsive to the presidential tasking.

4. The Committee found the ICA makes a clear argument that the manner and aggressiveness of the Russian interference was historically unprecedented. However, the ICA and its sources do not provide a substantial representation of Russian interference in

the 2008 and 2012 presidential elections, as the Committee understands was part of the President's original tasking.

5. [REDACTED] The Committee found that the ICA did not provide a set of policy on how to respond to future Russian active measures, which was part of the tasking the President conveyed to the Director of National Intelligence (DNI) James Clapper. The ICA did include, in the compartmented version, an unclassified section independently produced by DHS, FBI, and the Department of Commerce's National Institute of Standards and Technology (NIST), "DHS/FBI/NIST Recommendations: Options to Protect and Defend US Election Infrastructure and US Political Parties."

The absence of policy recommendations was deliberate, due to the well-established norm that the IC provides insight and warning to policy makers, but does not itself make policy.

6. The Committee found the ICA would benefit from a more comprehensive presentation of how Russian propaganda-as generated by Russia's multiple state-owned platforms-was used to complement the full Russian influence campaign.

Open source collection is a long-standing discipline for CIA and other elements of the IC, and open source reporting is used throughout the ICA to support specific analytic assertions. However, open source reporting on RT and Sputnik's coverage of WikiLeaks releases of Democratic National Committee (DNC) information would have strengthened the ICA's examination of Russia's use of propaganda. On this point, the Committee finds that Annex [REDACTED] of the ICA-"Open Source Center Analysis: Russia: Kremlin's TV Seeks to Influence Politics, Fuel Discontent in US," published December 12, 2012-should have been updated to provide a summary of Kremlin propaganda in 2016, thereby making a more relevant contribution to the ICA. An update to this assessment was not produced by the Open Source Enterprise until after the publication of the ICA.

7. [REDACTED] The role of social media has been a significant focus by the Committee and is discussed in a separate volume of this report.

State Department Statement on Cyber Attack on Czech Hospital

The U.S. government warns hackers in the latest of its public warnings for other nation states and hacking groups adhere to global cyber norms.

The Secretary of State Mike Pompeo issued a strongly worded statement, decrying reported cyber-attacks against the Czech Republic's healthcare system. In keeping with Trump Administration policy, Pompeo vowed that perpetrators would be held "accountable" and "should expect consequences" without any detail on what such U.S. actions would look like. However, the lack of a defined response may say less about U.S. resolve and more about using the power of ambiguity and uncertainty. And yet, this warning did not name a responsible country or entity, and it was issued as a statement by the Secretary whereas other, recent warnings were released as departmental statements.

In relevant part, Pompeo stated

> As the world battles the COVID-19 pandemic, malicious cyber activity that impairs the ability of hospitals and healthcare systems to deliver critical services could have deadly results. Anyone that engages in such an action should expect consequences.

Pompeo stated that "[w]e call upon the actor in question to refrain from carrying out disruptive malicious cyber activity against the Czech Republic's healthcare system or similar infrastructure elsewhere...[and] also call upon all states not to turn a blind eye to criminal or other organizations carrying out such activity from their territory."

Pompeo further explained

> The United States has zero tolerance for malicious cyber activity designed to undermine U.S. and international partners' efforts to protect, assist, and inform the public during this global pandemic. Such activity against critical civilian infrastructure is deeply irresponsible and dangerous. The United States promotes a framework of responsible state behavior in cyberspace, including nonbinding norms regarding states refraining from cyber activities that intentionally damage critical infrastructure and knowingly allowing their territory to be used for malicious cyber activities. When states do not abide by this framework, we hold them accountable.

This warning follows other Department of State warnings to nations conducting attacks. Earlier this month, the "Departments of State, Homeland Security, and Treasury, and the Federal Bureau of Investigation issued an advisory to raise the awareness of the cyber threat posed by North Korea... highlight[ing] North Korea's malicious cyber activities around the world, identifies U.S. government resources that provide technical and threat information, and includes recommended measures to counter the cyber threat" according to a press release.

In February, the Department of State also attributed a cyber-attack in the nation of Georgia to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST, aka Unit *74455* and Sandworm). The Department claimed GRU "carried out a widespread disruptive cyber attack [in 2019]...which directly affected the Georgian population, disrupted operations of several thousand Georgian government and privately-run websites and interrupted the broadcast of at least two major television stations." The Department added that "[t]his action contradicts Russia's attempts to claim it is a responsible actor in cyberspace and demonstrates a continuing pattern of reckless Russian GRU cyber operations against a number of countries." The U.S. called on "Russia to cease this behavior in Georgia and elsewhere."

These public statements by the Department are aligned with Trump Administration strategy regarding cyberspace. The September 2018 U.S. Cybersecurity Strategy identified a number of priority actions in the international space, including "Attribute and Deter Unacceptable Behavior in Cyberspace:"

> As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.

Conceivably, warning those attacking the health system of a North Atlantic Treaty Organization (NATO) ally like the Czech Republic would be an instance of deterrence.

Supreme Court to Hear CFAA Case

The U.S.'s top court takes on a statute that could criminalize violating terms of service. Currently, there are two different views among federal appeals courts, meaning one's criminal liability depends on where they are charged.

The Supreme Court of the United States (Court) will consider a case on the scope of the "Computer Fraud and Abuse Act" (CFAA) (18 U.S.C. § 1030). Specifically, the Court will rule on whether a person authorized to use part of a computer system is committing a crime when she accesses information on that system without authorization and with an improper purpose. Federal appellate courts have disagreed about what the term "exceeds authorized access" means in this context, and so the Court has the opportunity to define this term under the CFAA. This term could conceivably be used to punish people who violate the terms of service (TOS) for a service or website by lying about their identity or location. Consequently, the Court could determine how this key term in the CFAA should be applied and address the bigger question of whether any TOS violation set by a private company can lead to criminal liability or whether the CFAA may lead to criminal charges only if a person bypasses a clear barrier like a page that requires a passcode.

In *Van Buren v. United States*, the Court will consider the question of "[w]hether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose." In this case, the defendant was a police officer who took money as part of a sting operation to illegally use his access to Georgia's database of license plates to obtain information about a person. The Eleventh Circuit Court of Appeals denied his appeal of his conviction under the CFAA per a previous ruling in that circuit that "a defendant violates the CFAA not only when he obtains information that he has no "rightful[]" authorization whatsoever to acquire, but also when he obtains information "for a nonbusiness purpose."

According to the defendant's summary of the legal issues:

> The Computer Fraud and Abuse Act (CFAA)makes it a federal crime to "access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any protected computer." 18 U.S.C.§ 1030(a)(2)(C). Under the Act, to "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Id.§ 1030(e)(6).This case presents a recurring question about the interpretation of these provisions, on which the courts of appeals are openly divided: Does a person obtain information on a computer that he is "not entitled so to obtain" when he has permission to access the information, but does so for an improper purpose? The answer to this question has sweeping implications.

The defendant continued

> Accessing information on those computers is virtually always subject to conditions imposed by employers' policies, websites' terms of service, and other third-party restrictions. If, as some circuits hold, the CFAA effectively incorporates all of these limitations, then any trivial breach of such a condition—from checking sports scores at work to inflating one's height on a dating website—is a federal crime.

The Department of Justice argued

- Although some disagreement exists in the circuits about the meaning of the phrase "exceeds authorized access" in 18 U.S.C. 1030, this case would be a poor vehicle for resolving that issue because the decision below is interlocutory and because the jury instructions at petitioner's trial were consistent with petitioner's narrower interpretation of "exceeds authorized access. "Further review is therefore unwarranted.
- The petition does not otherwise warrant this Court's review. Congress has prohibited "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing]***information from any protected computer."18 U.S.C. 1030(a)(2)(C). And Congress has defined the phrase "'exceeds authorized access'" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."18 U.S.C. 1030(e)(6). Petitioner contends (Pet. 6) that a person exceeds authorized access only when "he had no right at all to access the information "he obtained, and argues (Pet. 6-7, 16-22) that the Eleventh Circuit's contrary reading of "exceeds authorized access" is too broad. But this case would be a poor vehicle for resolving any circuit disagreement about the scope of the statutory phrase "exceeds authorized access."

So far there have been two briefs filed by interested parties (so-called amicus briefs). The National Association of Criminal Defense Lawyers argued that

- Computers are ubiquitous in daily life. It is important that the Court clarify that ordinary deviances from terms-of-use requirements—whether imposed by internet websites or private company use guidelines, to name but a few—are not criminal. For that reason, this Court should grant review. This Court's review also is necessary because the Eleventh Circuit's decision deviates from settled practices for construing federal criminal statutes.

The Electronic Frontier Foundation, Center for Democracy & Technology, and New America's Open Technology Institute filed the other brief and asserted

> As the CFAA has been increasingly invoked in both criminal and civil proceedings over the last fifteen years, courts have become split on key questions of the statute's scope. The disagreement between the courts has translated into widespread public confusion—the very outcome that the Rule of Lenity is supposed to prevent...It has also chilled important security research and investigations of discriminatory practices online.

The Court's ultimate ruling could conceivably be narrow and just address the question of whether a public servant using his otherwise authorized access to government systems to exceed their authorization runs afoul of the CFAA. In any event, a ruling in this case would come later this year at the earliest.

Regulations Revised To Stop Flow Of Technology Into PRC, Russia, and Venezuela

The Department of Commerce's Bureau of Industry and Security (BIS) has published two final rules and a proposed rule to tighten the United States' control of the exporting of items that are dual use (i.e. usable for both civilian and military purposes) to primarily the People's Republic of China even though Russia and Venezuela are also targeted by these actions. In the Department's press release, it was asserted that the "new export control actions to prevent efforts by entities in China, Russia, and Venezuela to acquire U.S. technology that could be used in development of weapons, military aircraft, or surveillance technology through civilian supply chains, or under civilian-use pretenses, for military end uses and military end-users."

The Department of Commerce continues its rewrite of U.S. export control regulations in the wake of the extensive reform of the U.S.'s regime to limit transfers of military and civilian technology with possible military uses.

In the first rule, BIS amended the "the Export Administration Regulations (EAR) to expand license requirements on exports, reexports, and transfers (in-country) of items intended for military end use or military end users in the People's Republic of China (China), Russia, or Venezuela." BIS explained the "rule expands the licensing requirements for China to include "military end users," in addition to "military end use"...[and] broadens the list of items for which the licensing requirements and review policy apply and expands the definition of 'military end use.'" BIS claimed the rule was issued "to support the national security and foreign policy objectives of the United States by broadening the United States government's visibility into and ability to deny or condition exports, reexports, and transfers (in-country) involving certain items on the Commerce Control List (CCL) (Supplement No. 1 to part 774 of the Export Administration Regulations) that are destined to military end users or end uses in China, Russia, or Venezuela."

In the second rule, BIS amended the "EAR by removing License Exception Civil End Users (CIV) and requiring a license for national security-controlled items on the CCL to countries of national security concern...[which] will advance U.S. national security interests by allowing U.S. government review of these transactions to these countries prior to export, reexport or transfer (in-country) in accordance with current licensing policy for national security-controlled items on the CCL."

In the proposed rule, "BIS is proposing to remove provisions which authorize reexports of certain national security-controlled items on the Commerce Control List (CCL) to gain better visibility into transactions of national security or foreign policy interest to the United States."

UK Opts Out of Google/Apple API

The British government has opted against using the Google/Apple app to trace and prevent the spread of COVID-19 and has instead opted for a coming app the National Health Service (NHS) will develop and operate. This decision comes a week after the Information Commissioner's Office (ICO) gave a qualified blessing to the Google/Apple effort. If the United Kingdom (UK) follows through on developing and utilizing its tracing app, it will

The British government will design and release its own contact tracing app to fight the spread of COVID-19 even though its data protection authority provisionally signed off on the Google/Apple API.

be moving against the current of most other European nations in opting not to use the Google/Apple approach. And yet, the NHS will utilize the expertise of the two tech giants in some capacity and will make available the "key security and privacy designs" of the app. In future iterations of the app, the NHS will allow British users to provide more data if they wish that the person would be able delete if they wish and will abide by the "Data Protection Act," the UK's governing law on privacy.

In a blog posting on April 24, the NHS explained "[i]n the coming weeks, the NHS will be launching a contact-tracing app...[that] automates the process of contact tracing - with the goal of reducing transmission of the virus by alerting people who may have been exposed so they can take action to protect themselves, the people they care about and the NHS."

The NHS added

- The app will give the public a simple way to make a difference and to help keep themselves and their families safe.
- The technology is based on research evidence developed by epidemiologists, mathematical modellers and ethicists at Oxford University's Nuffield Departments of Medicine and Population Health.
- Once you install the app, it will start logging the distance between your phone and other phones nearby that also have the app installed using Bluetooth Low Energy.
- This anonymous log of how close you are to others will be stored securely on your phone.
- If you become unwell with symptoms of COVID-19, you can choose to allow the app to inform the NHS which, subject to sophisticated risk analysis, will trigger an anonymous alert to those other app users with whom you came into significant contact over the previous few days.
- The app will advise you what action to take if you have been close to someone who has become symptomatic – including advising you to self-isolate if necessary.

The NHS explained

- In future releases of the app, people will be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends. Those of us who agree to provide this extra information will be playing a key role in providing additional information about the spread of COVID-19 that will contribute towards protecting the health of others and getting the country back to normal in a controlled way, as restrictions ease.
- The data will only ever be used for NHS care, management, evaluation and research. You will always be able to delete the app and all associated data whenever you want. We will always comply with the law around the use of your data, including the Data Protection Act and will explain how we intend to use it. We will be totally open and transparent about your choices in the app and what they mean. If we make any changes to how the app works over time, we will explain in plain English why those changes were made and what they mean for you. Your privacy is crucial to the NHS, and so while these are unusual times, we are acutely aware of our obligations to you. Just as the NHS strives at all times to keep your health records confidential, so it will keep the app data secure. Patient confidentiality is built in to the NHS. It is one of our key values.

The NHS claimed that "[w]e have prioritised security and privacy in all stages of the app's development, starting with the initial design, and user testing...[and] have drawn on expertise from across government and industry to review our design and help test the app." The NHS

revealed that "[w]e are working with Apple and Google on their welcome support for tracing apps around the world." The NHS stated that "[a]s part of our commitment to transparency, we will be publishing the key security and privacy designs alongside the source code so privacy experts can "look under the bonnet" and help us ensure the security is absolutely world class."

The NHS chose to develop its own app instead of using the Google/Apple app even though the UK's data protection authority gave the tech giants a positive assessment. On April 17, the United Kingdom's (UK) Information Commissioner's Office (ICO) released its opinion that "sets out the Commissioner's current thinking regarding a joint initiative by Apple and Google (which we are calling the Contact Tracing Framework (CTF)) to enable the use of Bluetooth technology to help governments and public health authorities (PHAs) reduce the spread of the virus."

The ICO stated

> The CTF is not itself a contact tracing app, and Google and Apple are not yet proposing to build such an app, although they have indicated that they intend to develop more functionality into their solution. For now, the aim is to enable third parties, such as PHAs, to create contact tracing apps that exchange information via Bluetooth Low Energy between devices.

The ICO found

- The proposals for the CTF itself appear aligned with the principles of data protection by design and by default. This is based on the understanding that the CTF is designed to:
    - only generate a limited amount of data from the user's device, that is then made available via the CTF application programming interface (API). This data includes periodically-generated cryptographic tokens (we have used the term 'tokens' for clarity, noting that the Apple and Google documentation calls these numbers 'identifiers') created on that device, and stored tokens collected from nearby devices via Bluetooth. Tokens are not associated with other data that may further identify or locate the device user; and
    - support the use of these tokens as part of a specific methodology for contact tracing, through their upload from a COVID-19 diagnosed user to a central server and subsequent notification to other app users from that server, with this process only matching tokens stored on a particular device (with the match only occurring on the device), if it had been in the proximity of the diagnosed user's device.
- The CTF is therefore intended to support the development of apps that protect their users' identities, both before any risk of infection has been identified and when a COVID-19 infection notification is made via the app.
- However, it will be possible for those developing COVID-19 contact tracing apps – anticipated to be whitelisted PHAs and similar organisations – to design apps that use the CTF but also collect other data and use other techniques beyond those envisaged by the CTF.
- Organisations designing contact tracing apps are responsible for ensuring the app complies with data protection law where it processes personal data and the organisations are the controllers for that data. This is especially important because individuals may believe that the data protection by design and by default principles used in the development of the CTF extend to all aspects of a contact tracing app that is built to use the CTF, which may not necessarily be the case. If the app processes data outside the CTF's intended scope, then the controller should ensure it assesses the data protection

implications of this processing (along with any undertaken by way of the CTF) and ensure that the processing is fair and lawful. It is also crucial that the processing is transparent.

- The Commissioner notes that the CTF's underlying principles are similar to the proposed 'Decentralized Privacy-Preserving Proximity Tracing' ('DP-3T') system. While this Opinion is about the CTF, where these similarities exist the Commissioner's views are equally applicable to the DP-3T proposals.
- This is a fast moving and highly complex situation. Apple and Google have stated that they acknowledge the CTF initiative is an ongoing project, that will doubtless evolve over time. There are also plans for a 'Phase 2' of the work that could see additional functionality. The Commissioner will remain engaged in this work as it continues.

However, the Ada Lovelace Institute, "an independent research institute and deliberative body dedicated to ensuring that data and AI work for people and society," released a "rapid evidence review of the technical considerations and societal implications of using technology to transition from the COVID-19 crisis...with a view to supporting the Government and the NHS as it adopts technical solutions to aid in the transition from the COVID-19 crisis." The Institute also found that "premature deployment of ineffective apps could undermine public trust and confidence in the long-term, hampering the widespread uptake of tracking technologies which may be critical to their eventual success."

The Ada Lovelace Institute (Institute) found that "[t]here is an absence of evidence to support the immediate national deployment of symptom tracking applications, digital contact tracing applications and digital immunity certificates." The Institute found that "[w]hile the Government is right to explore non-clinical measures for transition, for national policy to rely on these apps, they would need to be able to:

1. Represent accurate information about infection or immunity
2. Demonstrate technical capabilities to support required functions
3. Address various practical issues for use, including meeting legal tests
4. Mitigate social risks and protect against exacerbating inequalities and vulnerabilities

The Institute stated that "[a]t present the evidence does not demonstrate that tools are able to address these four components adequately...[and] [w]e offer detailed evidence, and recommendations for each application in the report summary." The Institute recommended:

- Effective deployment of technology to support the transition from the crisis will be contingent on public trust and confidence, which can be strengthened through the establishment of two accountability mechanisms:
    - the Group of Advisors on Technology in Emergencies (GATE) to review evidence, advise on design and oversee implementation, similar to the expert group recently established by Canada's Chief Science Adviser; and
    - an independent oversight mechanism to conduct real-time scrutiny of policy formulation.
- Clear and comprehensive primary legislation should be advanced to regulate data processing in symptom tracking and digital contact tracing applications. Legislation should impose strict purpose, access and time limitations."

The Institute stated

- Until a robust and credible means of immunity testing is developed, focus should be on developing a comprehensive strategy around immunity that considers the deep societal implications of any immunity certification regime, rather than on developing digital

immunity certificates. Full and robust Parliamentary scrutiny and legislation will be crucial for any future regime of immunity testing and certification.

- Technical design choices should factor in privacy-by-design and accessibility features and should be buttressed by non-technical measures to account for digital exclusion.

EDPB Reiterates Views on Data Protection in the context of COVID-19

The European Data Protection Board (EDPB or Board) adopted a pair of guidelines to guide the European Commission and European Union members on developing apps to trace the contact those with COVID-19 may have had and also to address the processing of health data. The Board addressed these activities in the context of the General Data Protection Regulation (GDPR), the ePrivacy Directive, and other EU laws. The Board also released two letters sent to Members of the European Parliament regarding

"The global scientific community is racing against the clock to develop a COVID-19 vaccine or treatment. The EDPB confirms that the GDPR offers tools giving the best guarantees for international transfers of health data and is flexible enough to offer faster temporary solutions in the face of the urgent medical situation." EDPB Chair Andrea Jelinek

In a letter to a pair of Members, the Board reiterated its view that the EU's current regulatory structure allows for both appropriate responses to health crises like pandemics and the protection of personal data and other fundamental rights. The EDPB explained:

> The EDPB is aware that the COVID-19 outbreak is raising numerous questions concerning data protection and privacy issues, especially in the context of national Governments and private actors turning towards the use of data driven solutions to help fight the spread of the disease. In this context, I would like to highlight that data protection laws already take into account data processing operations necessary to contribute to the fight against an epidemic. Therefore, there is no need to lift GDPR provisions but just to observe them. The EDPB has already issued guidance on data protection and privacy issues in this current crisis, as have many of its Members. What public health authorities in the Member States are allowed to do depends on the tasks assigned to them by law. Similarly, what employers can do concerning their own staff depends largely on national labour laws. Notwithstanding any potential difference in these sector specific laws, as regards data protection matters, the EDPB has already published guidelines on the issues of geolocation and other tracing tools, as well as the processing of health data for research purposes in the context of the COVID-19 outbreak.

The EDPB also stated:

> It is of the utmost importance to preserve data protection principles even, and more importantly, in this difficult situation. The data protection principles (including lawfulness, transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation and security) not only guarantee the protection of fundamental rights of our citizens, in line with our common European values and democracies, but also create trust in the governments who are looking into post-confinement data driven measures.

As noted, the EDPB also released guidelines for processing health data. In the "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak," the EDPB stated that "legal questions concerning the use of health data pursuant to Article4(15) GDPR for such research purposes keep arising." The Board stated that "[t]he present guidelines aim to shed light on the most urgent of these questions such as the legal basis, the implementation of adequate safeguards for such processing of health data and the exercise of the data subject rights." The EDPB stressed its intention to develop "a further and more detailed guidance for the processing of health data for the purpose of scientific research...[as] part of the annual work plan of the EDPB."

The EDPB stated that "[d]ata protection rules (such as the GDPR) do not hinder measures taken in the fight against the COVID-19 pandemic." The Board claimed that "[t]he GDPR is a broad piece of legislation and provides for several provisions that allow to handle the processing of personal data for the purpose of scientific research connected to the COVID-19 pandemic in compliance with the fundamental rights to privacy and personal data protection." The Board stated that "[t]he GDPR also foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for these purposes of scientific research."

The EDPB identified "[t]he key findings of these guidelines are:

1. The GDPR provides special rules for the processing of health data for the purpose of scientific research that are also applicable in the context of the COVID-19 pandemic.
2. The national legislator of each Member State may enact specific laws pursuant to Article (9) (2) (i) and (j) GDPR to enable the processing of health data for scientific research purposes. The processing of health data for the purpose of scientific research must also be covered by one of the legal bases in Article 6 (1) GDPR. Therefore, the conditions and the extent for such processing varies depending on the enacted laws of the particular member state.
3. All enacted laws based on Article (9) (2) (i) and (j) GDPR must be interpreted in the light of the principles pursuant to Article 5 GDPR and in consideration of the jurisprudence of the ECJ. In particular, derogations and limitations in relation to the protection of data provided in Article 9 (2) (j) and Article 89 (2) GDPR must apply only in so far as is strictly necessary.
4. Considering the processing risks in the context of the COVID-19 outbreak, high emphasise must be put on compliance with Article 5 (1) (f), Article 32 (1) and Article 89 (1) GDPR. There must be an assessment if a DPIA pursuant to Article 35 GDPR has to be carried out.
5. Storage periods (timelines) shall be set and must be proportionate. In order to define such storage periods, criteria such as the length and the purpose of the research should be taken into account. National provisions may stipulate rules concerning the storage period as well and must therefore be considered.
6. In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights pursuant to Article 12 to 22 GDPR. However, Article 89 (2) GDPR allows the national legislator to restrict (some)of the data subject's rights as set in Chapter 3 of the GDPR. Because of this, the restrictions of the rights of data subjects may vary depending on the enacted laws of the particular Member State.
7. With respect to international transfers, in the absence of an adequacy decision pursuant to Article 45 (3) GDPR or appropriate safeguards pursuant to Article 46 GDPR, public

> authorities and private entities may rely upon the applicable derogations pursuant to Article 49 GDPR. However, the derogations of Article 49 GDPR do have exceptional character only.

The Board also turned to guidance on contact tracing as well. In the "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak the EDPB stated its firm belief that

> when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework.

The EDPB stated it "generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals." The EDPB stated that "[f]urthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures...[and] [t]he general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19."

The EDPB explained that "[t]hese guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

- using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures;
- contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.

The EDPB stressed "that the GDPR and Directive 2002/58/EC (the "ePrivacy Directive") both contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the SARS-CoV-2 virus2." The Board reiterated it "has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users."

The EDPB, however, warned

- The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the "ratchet effect". It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.
- The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for

health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.

Court Approves FTC's $5 Billion Settlement with Facebook

Last week, a federal court approved the Federal Trade Commission's (FTC) July 2019 $5 billion settlement with Facebook arising from violations of the 2012 settlement regarding its relationship with from its partnership with Cambridge Analytica during the 2016 election. However, the FTC was not unanimous. In approving the settlement, the FTC split along partisan lines 3-2 with the two Democratic Commissioners voting against the settlement.

The largest settlement with the FTC for privacy and data security violations is finalized with Facebook facing years of complying with its terms and risking future fines or other action for violations.

The Court explained

> In the Court's view, the unscrupulous way in which the United States alleges Facebook violated both the law and the administrative order is stunning. And these allegations, and the briefs of some amici, call into question the adequacy of laws governing how technology companies that collect and monetize Americans' personal information must treat that information. But those concerns are largely for Congress; they are not relevant here. Mindful of its proper role, and especially considering the deference to which the Executive's enforcement discretion is entitled, the Court will grant the consent motion and enter the order as proposed.

In his statements about the settlement when announced last year, FTC Chair Joseph Simons explained that

> Today's complaint alleges that Facebook violated the Commission's order in three ways. First, we allege that Facebook told consumers that they could limit the sharing of their information to groups—their "friends," for example—but, in fact, Facebook shared the information more broadly with app developers. Second, we allege that Facebook did not adequately assess and address privacy risks posed by third-party app developers. Third, we allege that Facebook misrepresented to certain users that they would have to "turn on" facial recognition technology, but for millions of users, that technology was "on" by default. In addition to these alleged order violations, we also allege that Facebook violated the FTC Act when it told users it would collect their phone numbers to enable a security feature, but did not disclose that it also used those numbers for advertising purposes.

Simons outlined the structure of the settlement:

> The settlement with Facebook is based on the recommendation of the FTC's career enforcement staff, and includes three major components. First, Facebook must pay a $5 billion civil penalty, one of the largest in corporate history. Second, the order subjects the company to new, expanded privacy requirements. Third, the order imposes significant structural reforms on how Facebook does business, including greater corporate accountability, more rigorous compliance monitoring, and increased transparency.

In his dissenting statement, Commissioner Rohit Chopra listed his reasons for breaking with the FTC on the Google settlement:

- Facebook's violations were a direct result of the company's behavioral advertising business model. The proposed settlement does little to change the business model or practices that led to the recidivism.
- The $5 billion penalty is less than Facebook's exposure from its illegal conduct, given its financial gains.
- The proposed settlement lets Facebook off the hook for unspecified violations.
- The grant of immunity for Facebook's officers and directors is a giveaway.
- The case against Facebook is about more than just privacy – it is also about the power to control and manipulate.

Commissioner Rebecca Kelly Slaughter explained in her dissent that "[m]y principal objections are:

> (1) The negotiated civil penalty is insufficient under the applicable statutory factors we are charged with weighing for order violators: injury to the public, ability to pay, eliminating the benefits derived from the violation, and vindicating the authority of the FTC.
> (2) While the order includes some encouraging injunctive relief, I am skeptical that its terms will have a meaningful disciplining effect on how Facebook treats data and privacy. Specifically, I cannot view the order as adequately deterrent without both meaningful limitations on how Facebook collects, uses, and shares data and public transparency regarding Facebook's data use and order compliance.
> (3) Finally, my deepest concern with this order is that its release of Facebook and its officers from legal liability is far too broad.

She added that "[r]ather than accepting this settlement, I believe we should have initiated litigation against Facebook and its CEO Mark Zuckerberg…[and] [t]he Commission would better serve the public interest and be more likely to effectively change Facebook by fighting for the right outcome in a public court of law."

To put Facebook's $5 billion settlement in perspective, the company announced earnings on July 24, 2019 of $16.9 billion for the second quarter of 2019 and an overall profit of $22 billion in 2018. Additionally, the company budgeted for the $5 billion settlement by writing down $3 billion in the first quarter of 2019, meaning that the second quarter charge would be only $2 billion.

USTR Identifies Alleged Bad Actors Regarding IP Property Rights, Counterfeiting, and Piracy

The Trump Administration's top trade official calls out international bad actors regarding intellectual property theft, piracy, and counterfeiting.

Office of the United States Trade Representative (USTR) released "its annual Special 301 Report on the adequacy and effectiveness of trading partners' protection of intellectual property rights and the findings of its Review of Notorious Markets for Counterfeiting and Piracy (the Review), which highlights online and physical markets that reportedly engage in and facilitate substantial trademark counterfeiting and copyright piracy." However, if a nation or entity is

named in either report, it does not necessarily mean the Trump Administration will act against it. Rather, much of the impacts in these reports is in their "naming and shaming" function and a number of entities voluntarily vow to curb or eliminate the decried activities.

In the Special 301 Report, the USTR explained

> A top trade priority for the Administration is to use all possible sources of leverage to encourage other countries to open their markets to U.S. exports of goods and services and to provide adequate and effective protection and enforcement of intellectual property (IP) rights. Toward this end, a key objective of the Administration's trade policy is ensuring that U.S. owners of IP have a full and fair opportunity to use and profit from their IP around the globe. The Special 301 Report (Report) is the result of an annual review of the state of IP protection and enforcement in U.S. trading partners around the world...

The USTR added

- This Report provides an opportunity to call out foreign countries and to expose the laws, policies, and practices that fail to provide adequate and effective IP protection and enforcement for U.S. inventors, creators, brands, manufacturers, and service providers. The identification of the countries and IP-related market access barriers in the Report and of steps necessary to address those barriers are a critical component of the Administration's aggressive efforts to defend Americans from harmful IP-related trade barriers.
- Specifically, this Administration continues to closely monitor developments in, and to engage with, those countries that have been on the Priority Watch List for multiple years. Over the coming weeks, USTR will review the developments against the benchmarks established in the Special 301 action plans for those countries. For countries failing to address U.S. concerns, USTR will take appropriate actions, which may include enforcement actions under Section 301 of the Trade Act or pursuant to World Trade Organization (WTO) or other trade agreement dispute settlement procedures.
- The Report identifies foreign trading partners where IP protection and enforcement has deteriorated or remained at inadequate levels and where U.S. persons who rely on IP protection have difficulty with fair and equitable market access.

Among the nations flagged, the USTR listed the People's Republic of China and India first:

- USTR continues to place China on the Priority Watch List and Section 306 monitoring remains in effect. China's placement on the Priority Watch List reflects U.S. concerns with China's system of pressuring and coercing technology transfer, and the continued need for fundamental structural changes to strengthen IP protection and enforcement, including as to trade secret theft, obstacles to protecting trademarks, online piracy and counterfeiting, the high-volume manufacturing and export of counterfeit goods, and impediments to pharmaceutical innovation. Under Section 301 of the Trade Act of 1974, USTR has taken action to address a range of unfair and harmful Chinese acts, policies, and practices related to technology transfer, IP, and innovation. USTR also initiated dispute settlement proceedings at the WTO to address discriminatory licensing practices. Structural impediments to administrative, civil, and criminal enforcement continue to undermine IP protections, as do certain information communications technology (ICT), IP-ownership, and research and development localization requirements. Over the past year, the United States' engagement of China began to demonstrate key progress with the signing of the U.S. –China Economic and Trade Agreement in January 2020. The agreement requires changes in China's acts, policies, and practices, including structural reforms and other

changes to China's legal and regulatory regime to address numerous longstanding concerns of a wide range of U.S. industries.

- USTR identifies India on the Priority Watch List for lack of sufficient measurable improvements to its IP framework on long-standing and new challenges that have negatively affected U.S. right holders over the past year. Long-standing IP challenges facing U.S. businesses in India include those which make it difficult for innovators to receive, maintain, and enforce patents in India, particularly for pharmaceuticals; ineffectual enforcement activities, copyright4policies that fail to incentivize the creation and commercialization of content, and an outdated and insufficient trade secrets legal framework. In addition to these long-standing concerns, India also further restricted the transparency of information provided on state-issued pharmaceutical manufacturing licenses, continues to apply restrictive patentability criteria to reject pharmaceutical patents, and still has not established an effective system for protecting against the unfair commercial use, as well as the unauthorized disclosure, of undisclosed test or other data generated to obtain marketing approval for pharmaceuticals and certain agricultural chemical products.

In the Review of Notorious Markets for Counterfeiting and Piracy, the USTR stated

> Commercial-scale copyright piracy and trademark counterfeiting1cause significant financial losses for U.S. right holders and legitimate businesses, undermine critical U.S. comparative advantages in innovation and creativity to the detriment of American workers, and pose significant risks to consumer health and safety. The Notorious Markets List (NML) highlights prominent and illustrative examples of online and physical markets that reportedly engage in or facilitate substantial piracy or counterfeiting. A goal of the NML is to motivate appropriate action by the private sector and governments to reduce piracy and counterfeiting.

USTR stated that it

> highlights the following markets because they exemplify global counterfeiting and piracy concerns and because the scale of infringing activity in these markets can cause significant harm to U.S. intellectual property (IP) owners, consumers, legitimate online platforms, and the economy. Some of the identified markets reportedly host a combination of legitimate and unauthorized activities. Others openly or reportedly exist solely to engage in or facilitate unauthorized activity. This year's NML includes several previously-identified markets because owners, operators, and governments failed to address the stated concerns. Other previously-identified markets may not appear in the NML for a variety of reasons, including that: the market has closed or its popularity or significance has diminished; enforcement or voluntary action has significantly reduced the prevalence of IP-infringing goods or services; market owners or operators are cooperating with right holders or government authorities to address infringement; or the market is no longer a noteworthy example of its kind. In some cases, online markets in the 2018 NML are not highlighted this year but improvements are still needed, and the United States may continue to raise concerns related to these markets on a bilateral basis with the relevant countries.

The USTR added

The 2019 Notorious Markets List identifies examples of various technologies, obfuscation methods, revenue models, and consumer harms associated with infringing activity. USTR based its selections not on specific types of technologies but on whether the owners, operators, or users of a nominated market or affiliated network of markets reportedly engage in or facilitate substantial piracy or counterfeiting to the detriment of U.S. creators and companies. Those who submitted public comments this year highlighted the complex ecosystem that is abused by providers of pirated content, including domain name registrars, reverse proxy services, hosting providers, caching services, advertisers and ad placement networks, payment processors, social networks, and search engines. Each component in this ecosystem can play a role in facilitating or reducing piracy. For example, as noted above, last year's notorious market MP3va saw a significant decline in popularity due to actions by U.S. payment processors to stop accepting payments from the site. Additionally, for the first time this year, an ad placement network, Propeller Ads, is identified as a notorious market for its role in funding piracy websites. This year's review process also identified a growing concern about the proliferation of counterfeits facilitated by social media platforms. For example, right holders have expressed increasing concerns with a growing trend of counterfeit products being offered for sale on e-commerce features related to large platforms, such as WeChat. USTR will further study and monitor these concerns. Platforms can begin to address these concerns by establishing industry-standard IP enforcement policies, increasing transparency and collaboration with right holders to quickly address complaints, and working with law enforcement to identify IP violators.

GAO Finds Fault With Agencies' Cybersecurity

In a pair of reports, the Government Accountability (GAO) found a range of security flaws with two of the agencies charged with overseeing the cybersecurity of sectors of the U.S. economy.

The GAO released a public version of its September 2019 assessment of the Federal Communications Commission's (FCC) cybersecurity after a 2017 crash of its comment system during the comment period for the repeal of the Obama Administration's Open Internet Order (aka net neutrality).

"The global scientific community is racing against the clock to develop a COVID-19 vaccine or treatment. The EDPB confirms that the GDPR offers tools giving the best guarantees for international transfers of health data and is flexible enough to offer faster temporary solutions in the face of the urgent medical situation." EDPB Chair Andrea Jelinek

The GAO noted that as it "reported in September 2019, the FCC bolstered the capacity and performance of the Electronic Comment Filing System (ECFS) to reduce the risk of future service disruptions...[and] also implemented numerous information security program and technical controls for three systems that were intended to safeguard the confidentiality, integrity, and availability of its information systems and information." The GAO, however, "identified program and control deficiencies in the core security functions related to identifying risk, protecting systems from threats and vulnerabilities, detecting and responding to cyber security events, and recovering system operations...[and] made 136 recommendations to address these deficiencies." The GAO found that "[a]s of November 2019, FCC had made significant progress

in resolving many security deficiencies by fully implementing 85 (about 63 percent) of the 136 recommendations GAO made in September 2019...[and] had also partially implemented 10, but had not started to implement the remaining 41 recommendations."

In its priority recommendations to the Department of Homeland Security (DHS), the GAO flagged unfulfilled cybersecurity recommendations:

- In February 2017, we recommended that DHS establish metrics for assessing the National Cybersecurity and Communications Integration Center's adherence to applicable principles in carrying out statutorily-required cybersecurity functions. In addition, we recommended that DHS establish methods for monitoring the implementation of cybersecurity functions against the principles on an ongoing basis. The department has since taken action, but needs to complete several actions that are intended to address these recommendations. For example, DHS stated that it continues to determine the applicability of key performance indicators and performance targets.
- To facilitate adoption of the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, in February 2018, we recommended that DHS take steps to consult with respective sector partners, such as the sector coordinating councils, and NIST, as appropriate, to develop methods for determining the level and type of adoption of the Framework by entities across their respective sectors.
- As of January 2020, the department had begun taking steps to develop methods to determine the level and type of framework adoption in the respective sectors. Specifically, in October 2019, DHS, in coordination with its Information Technology (IT) sector partner, administered a survey to all small and midsized IT sector organizations to gather information on, among other things, framework use and plans to report on the results in 2020. DHS officials stated that any small or mid-sized business across all critical infrastructure sectors could complete the survey and that the department had promoted the survey to all sectors. While the department has ongoing initiatives, implementing our recommendations to gain a more comprehensive understanding of the framework's use by critical infrastructure sectors is essential to the success of protection efforts.
- In March 2019, we recommended that DHS take steps to ensure that positions in the 2210 IT management occupational series are assigned appropriate cybersecurity work role codes and assess the accuracy of position descriptions. DHS concurred with our recommendation. DHS conducted an audit of its components' cybersecurity coding efforts in fiscal year 2018 and identified actions that components needed to take to complete the assignment of appropriate cybersecurity work role codes and assess the accuracy of position descriptions. As of January2020, DHS was conducting a second audit for fiscal year 2019 which it estimates will be completed by June 30, 2020.
- In July 2019, we recommended that DHS develop a cybersecurity risk management strategy that includes the key elements called for in federal guidance and establish and document a process for coordination between its cybersecurity risk management and enterprise risk management functions. DHS concurred with our recommendations. In January 2020, DHS described steps it plans to take to implement these recommendations, such as developing an enterprise-wide cybersecurity risk management strategy and clarifying cybersecurity roles and responsibilities for coordination with offices responsible for enterprise risk management. DHS estimated that it would complete these actions by July 31, 2020.

Further Reading

- "Australia Is Going To Make Facebook And Google Pay For The Journalism They Use" – *BuzzFeed News* and "French publishers win decisive battle against Google" – *Politico EU*. Australia's Treasurer Josh Frydenberg explained in an op-ed that because Facebook and Google have not come to an agreement with the Australian Competition & Consumer Commission in "facilitat[ing] the development of a voluntary code of conduct governing the relationships between digital platforms and media businesses, the goal of which was to protect consumers, improve transparency and address the power imbalance between the parties." Frydenberg is threatening to put in place a system under which the Australian government would force these companies to pay journalism outlets for using their content. The Australian government could release a mandatory code by July followed by legislation. France's Autorité de la Concurrence has ordered Google to negotiate
- "Amazon used data from its sellers to create competing products: report" – *The Hill*. According to 20 former Amazon employees, the company is using data on products third parties sell on its platform to develop competing products contrary to the company's frequent claims. These claims will surely be scrutinized by the U.S. Department of Justice, the Federal Trade Commission, the European Commission, and the House Judiciary Committee, all of which are already investigating the company.
- "Vietnam says accusations it hacked China for virus information 'baseless'" – *Reuters*; "Vietnam alleged to have hacked Chinese organisations in charge of COVID-19 response" – *The Register*; "COVID-19 prompts Vietnam hackers to hit China health officials for info, say researchers" – CNET; and "Vietnam denies hacking Chinese organisations for coronavirus information" – *South China Morning Post*. Cybersecurity company, FireEye, released a report claiming in January Vietnam's APT32 started trying to hack into the People's Republic of China's Ministry of Emergency Management and the government of Wuhan province looking for information on how the COVID-19 pandemic started. To no great surprise, Vietnam denied the reports.
- "Investors Bet Giant Companies Will Dominate After Crisis" – *The New York Times*. The COVID-19 pandemic may exacerbate and accelerate the growth and dominance of companies like Amazon and Apple. It may also result in more focus in Congress on antitrust and anti-competitive issues.
- "Exam anxiety: how remote test-proctoring is creeping students out" – *The Verge*. The online proctor business has boomed during the COVID-19 pandemic as universities and colleges are turning to these services to police the taking of exams by students. However, it is not clear these companies have the privacy, cybersecurity, and technological policies in place to allay fears among students and some educators.
- "A Scramble for Virus Apps That Do No Harm" – *The New York Times*. Governments around the world are pushing into use a range of different smartphone apps to track people with COVID-19 and with whom they may have interacted. However, a number of problems remain, including privacy, cybersecurity, whether governments should be allowed to access Bluetooth, location data, and people's contacts. It is also proving a problem that in many place people are mostly not downloading the app. For example, Norway is on the high side of adoption at 30% of the population, a level that is far short of what is needed according to most conceptions of how this technology would ideally work. Some governments are looking at apps as part of their response.
- "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates" – *The New York Times*. There are many critics of the General Data Protection Regulation, arguing the nearly two-year data processing regime has largely been a failure. The reasons for these perceived shortcomings include enforcement is fractured among the European Union's

member nation's data protection authorities (DPA), the relatively small budgets of these agencies, the years of appeals of decisions, the complexity of the issues posed by the cases, the number of complaints, and the over-sized role of Ireland's DPA given that most tech giants have their European headquarters there. However, a number of ruling are expected this summer that may change views on the efficacy of the law.

- "Movie and TV Piracy Sees an 'Unprecedented' Spike During Quarantine" – *VICE*. As streaming services like Netflix are seeing surges in usage with significant parts of the world under various orders keeping people home, to no great surprise, illegal viewing has also exploded. However, the increase in the latter activities has jumped between 30-50% depending on the nation.