SECRECY ORDERS AND PROSECUTING LEAKS: POTENTIAL LEGISLATIVE RESPONSES TO DETER PROSECUTORIAL ABUSE OF POWER

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

WEDNESDAY, JUNE 30, 2021

Serial No. 117–31

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
48–313 WASHINGTON : 2022

COMMITTEE ON THE JUDICIARY

JERROLD NADLER, New York, *Chair*
MADELEINE DEAN, Pennsylvania, *Vice-Chair*

ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
HAKEEM S. JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
JAMIE RASKIN, Maryland
PRAMILA JAYAPAL, Washington
VAL BUTLER DEMINGS, Florida
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
SYLVIA R. GARCIA, Texas
JOE NEGUSE, Colorado
LUCY McBATH, Georgia
GREG STANTON, Arizona
VERONICA ESCOBAR, Texas
MONDAIRE JONES, New York
DEBORAH ROSS, North Carolina
CORI BUSH, Missouri

JIM JORDAN, Ohio, *Ranking Member*
STEVE CHABOT, Ohio
LOUIE GOHMERT, Texas
DARRELL ISSA, California
KEN BUCK, Colorado
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona
TOM McCLINTOCK, California
W. GREG STEUBE, Florida
TOM TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
DAN BISHOP, North Carolina
MICHELLE FISCHBACH, Minnesota
VICTORIA SPARTZ, Indiana
SCOTT FITZGERALD, Wisconsin
CLIFF BENTZ, Oregon
BURGESS OWENS, Utah

PERRY APELBAUM, *Majority Staff Director and Chief Counsel*
CHRISTOPHER HIXON, *Minority Staff Director*

C O N T E N T S

WEDNESDAY, JUNE 30, 2021

SECRECY ORDERS AND PROSECUTING LEAKS: POTENTIAL LEGISLATIVE RESPONSES TO DETER PROSECUTORIAL ABUSE OF POWER

Wednesday, June 30, 2021

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to call, at 10:08 a.m., in Room 2141, Rayburn House Office Building, Hon. Jerrold Nadler [Chair of the Committee] presiding.

Present: Representatives Nadler, Lofgren, Jackson Lee, Cohen, Johnson of Georgia, Bass, Jeffries, Cicilline, Swalwell, Lieu, Raskin, Jayapal, Demings, Scanlon, Garcia, McBath, Stanton, Dean, Escobar, Jones, Ross, Bush, Jordan, Chabot, Buck, Gaetz, Johnson of Louisiana, Biggs, McClintock, Massie, Bishop, Fischbach, Spartz, Fitzgerald, Bentz, and Owens.

Staff Present: Aaron Hiller, Deputy Chief Counsel; Arya Hariharan, Chief Oversight Counsel; John Doty, Senior Advisor; Moh Sharma, Director of Member Services & Outreach and Policy Advisor; Jacqui Kappler, Oversight Counsel; Priyanka Mara, Professional Staff Member and Legislative Aide; Cierra Fontenot, Chief Clerk; Gabriel Barnett, Staff Assistant; Ben Hernandez-Stern, Counsel, Subcommittee on Crime, Terrorism, and Homeland Security; Ken David, Minority Counsel; Sarah Trentman, Minority Senior Professional Staff Member; Michael Koren, Minority Senior Professional Staff Member; and Kiley Bidelman, Minority Clerk.

Chair NADLER. The House Committee on the Judiciary will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on "Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power."

Before we begin, I would like to remind Members that we have established an email address and distribution list dedicated to circulating exhibits, motions, or other written materials that Members may want to offer as part of our hearing today. If you would like to submit materials, please send them to the email address that has been previously distributed to your offices, and we will circulate the materials to Members and staff as quickly as we can.

For those in the room, current guidance from the Office of the Attending Physician is that individuals who are fully vaccinated for COVID–19 do not need to wear a mask or maintain social distancing. Fully vaccinated individuals may of course choose to continue wearing masks based on their specific risk considerations. If you are not fully vaccinated, the Office of the Attending Physician requires you to wear a mask and maintain six feet of social distance.

Finally, I ask all Members, both those in person and those appearing remotely, to mute your microphones when you are not speaking. This will help prevent feedback and other technical issues. You may unmute yourself anytime you seek recognition.

I will now recognize myself for an opening statement.

On May 7th, 2021, *The Washington Post* reported that the Trump Administration secretly obtained phone records and had sought email records of certain of its reporters. Later reports showed that the department made similar attempts to access the communications records of a CNN reporter and multiple journalists at *The New York Times*.

On June 10th, it was reported that the Trump Administration had also requested the records of multiple Members of Congress, their family members, and congressional staff. On June 13th, *The New York Times* reported that the Trump Administration had sought similar records from accounts associated with former White House counsel Don McGahn.

Even if that were the end of the story, if all the Department had done was target these reporters and these Members of Congress this one time, we would have reason to be concerned. A free press is vital to our democratic system, and the Constitution grants extraordinary protections to the official communications of Members of Congress and their staff.

Of course, these reports do not constitute an isolated incident. The Department of Justice has a long history of targeting reporters and misusing its surveillance authorities to bypass basic constitutional protections. President Nixon's Justice Department tried to silence the publication of the Pentagon Papers. President Bush's Justice Department went after the reporters who helped expose the NSA's expansive warrantless surveillance programs. President Obama's Justice Department went so far as to charge a reporter as a co-conspirator in violation of the Espionage Act. President Trump's Justice Department appears to have targeted reporters and Members who were focused on investigating Russia's interference in the 2016 election. Now, we know that President Biden's Justice Department sought to renew at least some of the secrecy orders associated with these cases.

In each of these cases, the Department took advantage of outdated policies that make secrecy the norm, not the exception to the rule. In fact, these recent cases appear to have targeted journalists, Democratic Members of the House—of Congress, and the former White House counsel. We have no immediate way of knowing how big the problem is because each of these cases was accompanied by a DOJ-requested, judge-imposed gag order that prevents anybody from talking about them for years.

Now, we have asked the Department to explain the extent of these troubling cases. This hearing is not about that investigation, at least not directly.

Today, the Committee is going to focus on a related policy problem that has troubled Members on both sides of the aisle—namely, that technology has vastly outpaced the law when it comes to the government demanding your data from a third-party provider and that the gag orders accompanying those demands have become standard practice in cases where timely notice would make far more sense.

In the 21st century, Federal prosecutors no longer need to show up to your office; they just need to raid your virtual office. They do not have to subpoena journalists directly; they just need to go to the cloud. Rather than providing Americans with meaningful notice that their private electronic records are being accessed in a criminal investigation, the Department hides behind its ability to ask third-party providers directly.

They deny American citizens, companies, and institutions their basic day in court, and, instead, they gather their evidence entirely in secret. Just because it is easier for prosecutors to seek sweeping amounts of data from these service providers does not mean that they should be allowed to do so.

This Committee has long recognized the Justice Department's need to investigate the unauthorized disclosure of classified information, and it supports those investigations whenever they are properly predicated. Our responsibility to combat leaks is not, however, carte blanche authority to engage in sweeping surveillance of American citizens, businesses, newsrooms, and universities. It was not tolerable after 9/11, but it is not acceptable now.

If history and recent reporting has taught us anything, it is that we cannot trust the Department to police itself. It is imperative that the Committee fulfill its role and ensure our laws are keeping pace with rapidly changing technology. We need to guard against future overreach of Federal prosecutors by implementing reform now.

I thank our Witnesses for being here today. I look forward to hearing their ideas on what reforms we should consider moving forward, and I look forward to working with Mr. Jordan and our Republican colleagues on this matter.

I now recognize the Ranking Member of the Judiciary Committee, the gentleman from Ohio, Mr. Jordan, for his opening statement.

Mr. JORDAN. Thank you, Mr. Chair.

Mr. Chair, in the United States of America, the government should not spy on its citizens, plain and simple. In the limited cases when surveillance on Americans is necessary to prosecute crimes or prevent acts of terror, there should be a high burden, a very high burden, for the government in getting approval to do so.

What came out of the Church Committee's investigation into the FBI'S rogue actions in the middle of the 20th century provided a roadmap for righting the wrongs of domestic surveillance. An entire apparatus of checks and balances was set up to hold government accountable when it sought to invade the privacy of its citizens.

This process again is now in need of reform. The laws and guidelines governing surveillance are opaque, antiquated, and easily skirted. Our system of warrants, subpoenas, national security letters, secret courts, and other tools at the government's disposal must be brought in line with constitutional considerations of basic due process. We have tried to make progress in recent years, but we have much work left to do.

For instance, the USA FREEDOM Act made significant improvements to the PATRIOT Act to safeguard civil liberties, but many deficiencies remain, like the simple fact that the Obama FBI spied on President Trump's campaign, used a dossier that they knew to be false at the time to be able to surveil the activities of Carter Page. Further improvements are—quite frankly, a complete overhaul of FISA is something this Committee should again take up.

More recently, Tucker Carlson stated on his show the other night his belief that the NSA was monitoring his communications. While the NSA said in a carefully worded statement—and I would encourage all of you to read that Mr. Carlson was not a target, they didn't deny that they had reviewed his communications.

Additionally, reforms to the Electronic Communications Privacy Act, or ECPA, passed the House in two recent Congresses, only to stall in the United States Senate. As most of our colleagues know, ECPA is the cornerstone law governing Americans' privacy with respect to email and other electronic data. The problem is that this law was written in 1986 and did not contemplate, not even close to contemplate, all the facets of our digital age today. The result has been a patchwork system of demands from law enforcement to technology companies in a constitutionally dubious fashion. Courts are split, for instance, on how to interpret parts of ECPA, and this uncertainty allows for data to be swept up by law enforcement agencies without warrants.

Another area where we can work together is on protecting the public's right to know. An informed public is critical to a well-functioning democracy. When the Department of Justice prosecutes journalists or implements a gag order so that people cannot speak out about the government's actions, our democratic values are undermined. There are bipartisan bills that will protect journalist sources. This legislation was originally authored by Vice-President Pence when he was a Member of the House. We should revisit this legislation and measures related to gag orders so that the public can be as informed as possible. It should be incredibly rare in the United States that people are not allowed to speak freely about the government's actions.

I look forward to today's discussion, and, frankly, like the Chair said, "I'm optimistic about an opportunity to work with our colleagues on the other side to make some improvement in all these areas."

With that, Mr. Chair, I yield back.

Chair NADLER. Thank you, Mr. Jordan.

Without objection, all other opening statements will be included in the record.

Chair NADLER. I will now introduce today's Witnesses.

Eve Burton is an Executive Vice President and the Chief Legal Officer of the Hearst Corporation. Prior to joining Hearst, Ms. Bur-

ton served as Vice President and Chief Legal Counsel at CNN, where she oversaw all legal matters relating to news and other programming on CNN networks and websites. Previously, she was a Deputy General Counsel at the New York Daily News. She also clerked for Judge Leonard Sand in the United States District Court of New York. Ms. Burton holds a B.A. from Hampshire College and a J.D. from Columbia Law School.

Tom Burt is corporate Vice President for customer security and trust at Microsoft Corporation. Among his department's many responsibilities is responding to law enforcement requests for access to data and managing Microsoft's government clearance and national security compliance. Mr. Burt joined Microsoft in 1995 and has held several leadership roles in the corporate, external, and legal affairs departments. He received an A.B. from Stanford University and a J.D. from the University of Washington School of Law.

Jonathan Turley is the J.B. and Maurice C. Shapiro Professor of Public Interest Law at The George Washington University Law School. After a previous position teaching at Tulane Law School, Professor Turley joined the G.W. law faculty in 1990, and in 1998 he became the youngest chaired professor in the school's history. In addition to serving as counsel on a number of significant cases, he has written numerous articles for a variety of law journals and national publications. Professor Turley earned a B.A. from the University of Chicago and a J.D. from Northwestern University School of Law.

Lynn Oberlander is of counsel with the law firm of Ballard Spahr LLP. Previously, she served as In-House Counsel to numerous broadcasters, publishers, and digital platforms. She was a Senior Vice President and Associate General Counsel for media at Univision Communications, Inc., while also serving as Executive Vice President and General Counsel at Univision's subsidiary Gizmodo Media Group. Previously, she was the General Counsel for media operations at First Look Media Works, and before that she was the General Counsel of *The New Yorker*, where she also wrote for *newyorker.com* on media law topics. Earlier in her career, she also worked at Forbes and NBC. Ms. Oberlander received her B.A. from Yale University and her J.D. from Columbia Law School.

We welcome all our distinguished Witnesses, and we thank them for participating today.

I'll begin by swearing in our Witnesses. I ask that our Witnesses in person please rise and raise your right hand. I ask that our remote Witness please turn on her audio and make sure I can see your face and your raised right hand while I administer the oath.

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

Let the record show that the Witnesses have answered in the affirmative.

Thank you, and please be seated.

Please note that each of your written statements will be entered into the record in its entirety. Accordingly, I ask that you summarize your testimony in five minutes. To help you stay within that time limit, there is a timing light on your table. When the light

switches from green to yellow, you have one minute to conclude your testimony. When the light turns red, it signals your five minutes have expired. For our Witness appearing virtually, there is a timer on your screen to help you keep track of time.

Ms. Burton, you may begin.

TESTIMONY OF EVE BURTON

Ms. BURTON. Chair Nadler, Ranking Member Jordan, Members of the Committee, good morning. My name is Eve Burton. I am an executive vice President and the chief legal officer of the Hearst Corporation. I am pleased to appear before you today to discuss this critical issue.

This is not a partisan, political matter. It is not a concern limited to the press or the Congress. It is an American issue, and how we approach it will tell a lot about what kind of country we want to be.

I want to acknowledge the obvious. There is a natural tension between prosecutors' interest in exercising their investigative power and the individual's interest in protecting their constitutional rights, and these are difficult interests to balance.

That is the key: They must be balanced fairly and consistently. Our constitutional system requires that due process is accorded all citizens through the application of proper procedures that protect fundamental rights. With rare exceptions, these matters should not be decided in secret.

Recent revelations about the DOJ's use of its investigative powers to secretly obtain citizens' communications records directly from telephone and email providers should be of great concern to every American. We all rely on these services in our daily lives.

While we do not yet know all the details of how or why the DOJ went about this secret collection, enough facts have emerged to suggest that Congress should consider legislation to ensure appropriate balancing and adequate protection of individual rights in the future.

Congress has stepped in before to provide legislative protections for important rights as it did with the 1980 Privacy Protection Act. The PPA established strong procedures for news organizations to challenge search warrants of newsrooms, which were until then planned and executed in secret.

Congress should do more, especially where third-party communication companies are concerned. That is the principal unaddressed problem in 2021.

The aim of my testimony is to share my views on what should be central components of any legislative reform in this area. My written submission provides an expanded discussion of these necessary pieces, but I will summarize them here.

The single most important step and one that is steeped in our shared American values is to recognize the importance of due process and procedural safeguards. This could be done by codifying something like the DOJ subpoena guidelines. They lay out procedures to protect fundamental press rights from investigative power. This is a good baseline for legislation to address today's problems. The guidelines are just a starting point, and we must go forward.

Further, to that end, a critical second step is to recognize the necessary role of Article III Judges in balancing competing interests. The DOJ should not be prosecutor, judge, and jury when it comes to citizens' fundamental rights. The Department simply has an inherent conflict.

A third step is the establishment of procedures that specifically recognize the realities of modern communication technology. The same protections must apply whether the information is sought in an Office file or on a cloud server across the country or the world managed by Google, Microsoft, Apple, or Verizon.

These are not theoretical issues; they are practical issues. We must extend procedural protections to records stored with cloud companies, or else we may never know when our records are seized by the government.

Presently, the protection of our constitutional interests is in the hands of middlemen who have no incentive to battle with the government on behalf of customers or citizens. To the contrary, in my experience, some communication companies have historically seen it as their responsibility to assist the government in obtaining what it wants.

Finally, legislation should be clear there is a presumption against secrecy orders, and the government must bear the burden of overcoming that presumption. The Pentagon Papers case, decided exactly 50 years ago today, reminds us that prior restraints are rarely, if ever, constitutionally permissible, even when the government invokes national security concerns during wartime. This is the constitutional presumption against which gag orders must be judged.

I would like to close my testimony by reiterating my belief that much of our concern about prosecutorial abuse of investigative power can be addressed in a way that should not be controversial or interfere with legitimate government work.

Instead, I believe we can all agree that many of these concerns can be addressed with clear procedures that establish a presumption of openness, with notice and an opportunity to be heard, as the norm and the expectation. This assures that difficult questions about the balancing of constitutional interests that must occur will be properly decided by our great and independent judiciary.

I look forward to our discussion today and thank you all for the opportunity to participate in this hearing.

[The statement of Ms. Burton follows:]

TESTIMONY OF EVE BURTON

**EXECUTIVE VICE PRESIDENT AND CHIEF LEGAL OFFICER,
HEARST CORPORATION**

BEFORE

THE UNITED STATES HOUSE OF REPRESENTATIVES

JUDICIARY COMMITTEE

**"SECRECY ORDERS AND PROSECUTING LEAKS:
POTENTIAL LEGISLATIVE RESPONSE TO DETER PROSECUTORIAL
ABUSE OF POWER"**

JUNE 30, 2021

Chairman Nadler, Ranking Member Jordan, members of the Committee, good morning. My name is Eve Burton. I am an executive vice president and the chief legal officer of the Hearst Corporation, a leading global diversified media, information and services company, with more than 360 businesses, including 33 local television stations; dozens of newspapers including the Houston Chronicle, San Francisco Chronicle and the Albany Times Union, and hundreds of magazine titles.

I am pleased to appear before you today to discuss potential legislative approaches to address concerns arising from unchecked prosecutorial investigative power. This issue is not a partisan political issue. It is not an issue limited to the press or the Congress. It is an American issue, and our efforts in addressing it will tell a lot about what kind of country we want to be.

I would like to begin by acknowledging the obvious: that there is a natural tension between the government's interest in exercising its investigative power and the individual's interest in protecting constitutional rights. This is not a new tension, nor is it likely to be resolved conclusively by this or future generations. These are hard interests to balance. But that is the key – they are interests that must be balanced – fairly and consistently over time, in order to keep our Constitution strong.

And it is clear that the Department of Justice is not suited to do the balancing, nor is any other arm of the Executive branch. They are too vested in the outcome. The balancing must be done by our courts, which are independent and uniquely qualified to consider the competing claims of law enforcement and citizens whose constitutional rights are at stake. It is equally clear that those whose rights are at stake must have notice, so that they can appear in court and seek to protect those rights or have someone else who will. There simply cannot be routine government sanctioned secrecy in such cases. These are basic procedural guarantees that are grounded in fairness and due process, and are absolutely necessary if our constitutional rights are to mean anything in the face of a government investigation.

The fact that government investigations pose a threat to constitutional rights is not a matter for debate. Take the First Amendment rights of the press, for example. The Department of Justice itself recognized the significance of those rights, and the importance of yielding to them, in subpoena guidelines first adopted more than 50 years ago, when tensions between the press and

the government were at a high point. Those guidelines – which are still in effect – require the Department of Justice to balance its investigative needs against the press' strong First Amendment rights, and to obtain the Attorney General's personal sign-off on any subpoena seeking newsgathering or editorial materials from the press, creating a framework that meant subpoenas for press records are an investigative means of last resort to be used in only the rarest of cases. Justice White observed in his 1972 opinion in *Branzburg v. Hayes*, shortly after the guidelines were developed, that they held the promise "to resolve the bulk of disagreements and controversies between press and federal officials." And so they did. The self-regulatory approach reflected in those guidelines and their subsequent revisions worked relatively well for several decades, during which the Department of Justice exercised great restraint in pursuing the records of journalists.

But in recent years the approach has broken down and is no longer sufficient to protect the constitutional rights of journalists, much less members of Congress or other citizens. This is due in no small part to the evolution of communications technology, which has placed ever more of our everyday communications in the hands of third-party cloud and technology companies such as Google, Apple, Microsoft and Verizon. These companies pose an irresistible investigatory target, promising a trove of information, and one that avoids a direct request to individuals whose communications records are actually being sought. The breakdown is also due to an increased aggressiveness by DOJ in more cases to pursue those records it believes will advance its investigations, notwithstanding the rights on the other side of the balance.

One can readily see why self-regulation in this area no longer works; there is an inherent conflict. The DOJ is intensely interested in pursuing its investigative agenda, the records are too easy to obtain secretly under the current scheme, and competing rights are too easy to ignore. The DOJ cannot be the final arbiter of citizens' constitutional rights. This is why we urgently need legislative reforms that require effective notice, representation, and adjudication before an independent judiciary, separate and apart from the Department's compliance with its own procedures.

These are not theoretical issues. They are practical problems relevant to our daily work in informing the public. Hearst has dozens of newsrooms around the country and we are sensitive to the practical reality that with the rise of digital communication and cloud computing, and the

storage of records outside of the newsroom, one of the historic checks on prosecutorial power is weakened. If the government is not obligated to come to us directly to get our records, we may never have the opportunity to assert our rights to protect the information, and we may never even find out that our records were sought or obtained.

Subpoenas to newsrooms are not uncommon. We have received thousands over the years, mostly in the context of private litigation, but also from state and federal law enforcement. And in nearly all of those cases where a government agency seeks our newsgathering materials, we have been able to convince the government or have utilized the courts to quash these.

Government subpoenas certainly suggest an increased reliance on the press to serve as its investigative arm, but when we have notice of that intention, we can challenge what is wrong. It is the possibility that the government will bypass us entirely and go directly to technology and telecommunications companies that is most troubling. We can't see those requests when they happen in secret. In those cases, the protection of our interests is left in the hands of the middlemen communications companies that have little incentive to get into conflict with the government. In my experience, these companies have historically seen it as their responsibility to assist the government regarding anything it wanted. As one General Counsel told me "if my government asks for information, I do not question their motives. It is not my job to do so."

Here is one example. A few years ago, we learned that a telecommunications company turned over phone records of Hearst journalists as part of an investigation into the San Francisco Chronicle's reporting on a grand jury investigation into BALCO and the use of steroids in professional sports. Our reporting, which relied on confidential sources, was widely praised, including by President Bush. Yet the government wanted to know who the journalists' sources were, and waged parallel attacks: one, publicly, against our reporters directly, seeking to compel them to identify their sources, and a second, secretly, against their phone service provider. We know little about this second secret effort, which ended with some of our phone records being turned over. Years later, details of that effort remain secret. We don't even know whether the phone company resisted.

This dynamic of unaligned interests between media companies, cloud providers and the government has had a profound impact on many parts of our business. In part because of our

experience in the BALCO case, we have found it necessary to engage in tense contract negotiations with cloud providers over the need for notice and the right to challenge government requests for our records in open court. Our business is reporting information to the public and protecting information our journalists collect. Challenging misguided efforts by the government for access to that information is an imperative for us. Without legislative action requiring notice, judicial process and freedom from secret proceedings, we are left to rely only on trust in government and service providers. That does not inspire much comfort or confidence. Meaningful reform is long overdue in this area.

Recent revelations that the DOJ used secret subpoenas and gag orders to seek communications records from journalists and members of Congress is a continuation of these troubling trends and should be of great concern to every American. It shows the lack of any significant check on government prosecutorial power against the individual. Equally concerning is the DOJ's ability, and apparent routine willingness, to secretly use its investigative powers to obtain an individual's communications directly from communications service providers, such as the technology companies mentioned above, without so much as providing notice to the person whose communications are collected, much less the ability to challenge that subpoena in a court of law. The executive branch is playing the role of prosecutor, judge and jury, and disregards the important role our Constitution envisions for the co-equal branches of government in securing citizens' rights. In this march of the Article II Executive Branch, it has effectively claimed there is no role for our Article I Congress or our Article III judges. This lack of checks and balances is dangerous.

We do not yet know all the details of how or why the DOJ went about this secret collection of communications from the press, legislators, congressional staffers and others. The facts that have emerged so far suggest we are at an inflection point for Congress to consider adopting legislative safeguards that ensure appropriate balancing and adequate protection of constitutional rights. The aim of my testimony is to share what I think must be central components of any reform in this area.

The single most important step – and one that should be easy to agree on, based on our shared American values – is to recognize the importance of process, procedural safeguards and

transparency. This can be accomplished through legislation that codifies the procedures laid out in the DOJ subpoena guidelines. As I note below, these guidelines, while framed in the context of regulating subpoenas to the press, could form the basis for a legislated set of procedural protections for fundamental constitutionally protected conduct, not just for the press, but for members of Congress and the American public in the context where the government is using its prosecutorial investigative power. Those protections could also extend beyond the DOJ to all executive branch investigative and law enforcement agencies.

An equally uncontroversial second step is to recognize the role of Article III judges to balance competing interests. Consideration of such weighty matters of constitutional rights should not be left solely to the discretion of the very department that seeks to override such rights.

A third step is to establish procedures that recognize the realities of modern communications technology. Protections should be guaranteed to a person's communications regardless of where that information is stored. In other words, because information is in a cloud storage bin rather than in a file cabinet in the newsroom or at home, the government should have no greater investigative and secrecy interest due to the ease of access.

Finally, legislation should establish procedures governing those exceptional cases where the government can meet the necessarily high bar for seeking records in secret or with gag orders, where the party is not given notice and the opportunity to seek judicial review. This might include the establishment of panels of independent counsel qualified to advocate for constitutional interests. The key concept is to have some procedural method to get the issue before a court with someone representing the individual who might otherwise only find out about it months or years later, if ever.

As I hope will be clear in my testimony, I believe the primary answer is the establishment of strong and fair procedural protections with a presumption against secrecy, which should be limited to rare circumstances and only upon an affirmative showing of necessity by the government, applied narrowly and with a time limit. Once such protections are in place, many of the difficult questions can be left to the courts, which are uniquely empowered to balance precisely such competing and fundamental interests.

I.

I noted above that, in my view, these steps should be largely uncontroversial. Take, for example, the establishment of clear procedural protections and safeguards to ensure the balancing of constitutional interests. We all have individual constitutional rights that we cherish, and regardless of where we fall on the ideological or political spectrum, we also have an expectation that when our rights are challenged by the power of the government, federal prosecutors should not decide the question on their own. Indeed, the separation of powers that defines our system of governance provides for review of constitutional issues by the judiciary, which is uniquely well-suited to handle difficult balancing questions like these.

The DOJ has in some measure, over the five decades the guidelines have been in place, agreed on the importance of the rights at issue and the need for checks and balances – even if confined to its own agency – by expressly recognizing the legitimacy of its guidelines as a means to limit its investigative powers. These guidelines provide an excellent starting point for the discussion. While they are framed in the context of subpoenas to the news media, the guidelines, at their core, provide a series of procedures and safeguards designed to limit incursions on constitutionally protected conduct. They provide a basis to evaluate whether the investigative need is sufficient to overcome fundamental protections.

But guidelines lack the force of law and there is no right of standing to challenge the DOJ in court. The codification of the procedures embodied in these guidelines would clarify and limit the Department's use of subpoenas, and, of particular concern today, outline the procedures it must follow when it seeks to justify the use of secrecy to obtain constitutionally protected materials.

II.

Codification of these procedures should naturally include explicit recognition that, because we are concerned about the protection of constitutional interests, the proper administration of these procedures must be subject to independent judicial review. Article III judges can and should provide impartial oversight of the Department's investigative actions when they implicate constitutional interests. That oversight must include, except in the rarest of cases, notice to the individual and an opportunity to be heard, presumptively in an open court.

On occasion the DOJ has made clear that it views itself as the sole arbiter of its own conduct in applying these guidelines, deciding for itself whether it has done enough to balance its investigative interests against fundamental constitutional concerns.

This DOJ pushback against oversight was famously at the center of the 2006 Second Circuit decision in *New York Times v. Gonzales*, 459 F.3d 160 (2nd Cir., 2006). There, the Department approached a newspaper, seeking access to its phone records as part of an investigation into the leak of a not-yet executed government plan to freeze assets and search the premises of two organizations in connection with an investigation into funding of terrorist activities by organizations raising funds in the United States. When the newspaper declined to cooperate by providing the requested phone records, the Department threatened to seek the records directly from third party cloud service providers. The phone service providers declined the newspaper's request that it be notified if the government subpoenaed the records and that the newspaper be given an opportunity to challenge such action. And, when the same request for notice and an opportunity to object was put directly to the Department, it, too, rejected the notion that any such notice or opportunity to object was required.

As noted in the majority opinion in *Gonzales*, the Department asserted that it had "diligently pursued all reasonable alternatives out of regard for First Amendment concerns," and that it had "adhered scrupulously to Department policy." (*Gonzales*, 165). Despite these assurances, the Department rejected the notion that it had "an obligation to afford *The New York Times* an opportunity to challenge the obtaining of telephone records from a third party prior to its review of the records, especially in investigations in which the entity whose records are being subpoenaed chooses not to cooperate with the investigation." (*Gonzales*, 165). In an effort to be heard before the records were obtained, the *Times* filed a lawsuit seeking judicial review of the government's threatened actions and weighing of the important First Amendment interests at stake against the government's investigative interests.

Ultimately, the court ruled that whatever common law and First Amendment protections exist for journalists also protect their records when held by third party service providers, but that, on the facts presented, any such protections were overcome. Reasonable minds may disagree on the sufficiency of the government's evidence in that case, but the reason I raise this case today is

as an example of the value of judicial oversight of prosecutorial action. In *Gonzales*, as Judge Sack put it in his dissenting opinion, and a point on which all the judges agreed, was the court's clear affirmation that questions regarding the proper balancing of constitutional interests should be reviewed independently by the courts, not by the very agencies that seek to overcome those fundamental interests.

As Judge Sack wrote, the "question at the heart of" *Gonzales* was less about whether the information sought was subject to some constitutional protection, but rather which branch of government should decide whether such protection was overcome. In other words, the primary dispute was "not whether the plaintiff is protected in these circumstances, or what the government must demonstrate to overcome that protection, but to whom the demonstration must be made." (*Gonzales*, 176).

The government in *Gonzales* took the position that "federal courts have no role in monitoring its decisions as to how, when and from whom federal prosecutors or a federal grand jury can obtain information." (*Gonzales*, 176). That position was rejected because the Justice Department is not in a position to fairly and impartially evaluate when its own prosecutorial interests compete with the constitutional rights of those it is investigating.

As Judge Tatel noted in *In re Grand Jury, Judith Miller*, 438 F.3d 1141 (D.C. Cir. 2006), the executive branch "possesses no special expertise that would justify judicial deference to prosecutors' judgments about the relative magnitude of First Amendment interests. Assessing those interests," he continued, "traditionally falls within the competence of courts." (*In re Grand Jury*, 1175-76)

The codification of procedural protections governing the issuance of subpoenas should also ensure effective notice to those whose rights are at issue and an opportunity to be heard by an independent judiciary.

III.

These two steps – codification of procedures for issuance of subpoenas and impartial judicial review to ensure proper application of procedural and substantive safeguards – form the baseline for resolving concerns about abuse of investigatory power in seeking access to

constitutionally protected materials. But recent events make clear that in order to be effective, these procedural protections must also reflect the realities of modern communication and data storage.

In the past, the government might have sought an individual's communications by going directly to that person. Today, the government can, as it threatened to do in *Gonzales* and as it has done in many other cases (including those recently in the news), go directly to the companies that house those communications and seek to compel their production from those companies. This has perverse effects. First, it ignores the fact that these communications, whether stored in a person's home or on an email server in the cloud, still implicate the same fundamental constitutional interests. Second, particularly in those situations where no notice is given to the individual or where secrecy orders are used, it puts the third party communications service provider in the unenviable position of having to decide whether to turn over the materials or protect their customers in opposition to the government. That should not be their burden to bear. As I noted earlier, the technology companies have been clear for the most part that they do not want to be in the middle.

Congress can step in to correct this problem, much as it did with the federal Privacy Protection Act of 1980, a direct response to a Supreme Court decision that threatened to open the door to investigative searches of newsrooms. Two years earlier, the Supreme Court's decision in *Zurcher v. Stanford Daily* held that a newsroom could be searched as part of a criminal investigation as long as police had a valid search warrant. The decision sparked concerns that the government would view the decision as a license to convert the news media into an investigative arm of the government, and that it would chill investigative journalism on the actions of government. Congress stepped in quickly with the PPA, which established strong procedural protections for journalists against state and federal search warrants, allowing them the opportunity to challenge a search in court.

While the PPA provides robust procedural protection for journalists against a direct search of a newsroom, it falls short – as do the DOJ Guidelines – in protecting against an indirect search of records. To remedy this, the procedural safeguards discussed above should extend to requests for information that go to individuals' communications services providers – whether a telephone

company, email provider, cloud storage space, or other venues yet to be developed. This would recognize, as the *Gonzales* Court did, that whatever constitutional interests apply when an individual is subpoenaed directly must also extend to that individual's electronic records, even when in the hands of a third-party service provider. In most cases, this may be accomplished through notice to the individual whose records are being sought (preferably by the Department of Justice directly to the individual) and an opportunity to be heard by an Article III judge. Ideally, this would take the third-party service provider out of the middle in most circumstances, and would leave it to the individual, properly noticed, to defend their own interests in opposing a subpoena for their records from the outset.

Transparency is the key here. The secrecy orders that were placed on the press' lawyers most recently are another instance of prosecutorial overreach. The Pentagon Papers case, decided fifty years ago today, is a stark reminder that prior restraints are rarely, if ever, constitutionally permissible – even when the government invokes national security concerns. The recent gag orders placed on lawyers for the New York Times and CNN, which prevented them from communicating with and counseling their clients on the most urgent and important of all possible matters – government requests for their constitutionally protected editorial work product and source material – were egregious not only because they were prior restraints, but because they directly interfered with the attorney-client relationship, and those attorneys' ability to fulfill their professional responsibility to their clients. It prevented those attorneys from even notifying their clients that their rights were in danger. While the Department eventually agreed to loosen these unprecedented gag orders, by that time much damage had already been done to the rights of both the attorneys and their clients, and to the rule of law. Any legislation should clarify the extraordinary presumption against such secrecy orders, and the heavy burden the government must bear to justify one.

And for those rare circumstances where the Department might be able to satisfy a court that total secrecy is clearly justified, and where a court agrees that an individual cannot be given notice without causing grave harm to the integrity of the investigation, the procedures I believe are necessary should also include mechanisms to ensure that the individual's interests are in some way put before a judge by a competent representative. This might involve the development of independent panels of attorneys trained in the area of constitutional rights who could be called on

confidentially to stand in for the individual and represent their interests. Such panels might be agreed on contractually between individuals and their service providers at the outset of their contractual relationship, as some companies do already, but the public should not have to rely on their ability to privately negotiate such an arrangement with their telephone carrier or email service provider to ensure their rights are protected. For that reason, ideally, panels should be developed locally by courts themselves.

But the details of how such a system of confidential representation would be set up are secondary to the establishment of a procedural guarantee that even when a court order is obtained permitting the government to proceed with a request for protected materials without notifying the individual affected, the individual's constitutional interests will still be represented and an independent court will have the opportunity to review the government's purported need to override those interests.

I would like to close my testimony be reiterating my belief that much of our concern about prosecutorial abuse of investigative power can be addressed in a way that need not be politically controversial. Resolution of these issues need not be bogged down in discussions of who qualifies for judicial review, or what privileges against compelled discovery might apply to one group or another. Instead, I believe we can all agree that what matters most is, first, establishing a set of procedures governing the issuance of subpoenas that seek constitutionally protected materials, regardless of whether they are held by the individual or by a service provider, and, second, clearly establish a procedure for judicial review of such subpoenas, including in those rare circumstances where a court is satisfied that secrecy is warranted.

I look forward to our discussion today and I thank you for the opportunity to participate in this hearing.

Chair NADLER. Thank you for your testimony.
Mr. Burt, you may begin.

TESTIMONY OF TOM BURT

Mr. BURT. Chair Nadler, Ranking Member Jordan, and Members of the Committee, my team at Microsoft is responsible for responding to government data demands, so I appreciate the opportunity to testify on the need for legislative reform on secrecy orders.

While the recent news about secret investigations is shocking, most shocking is just how routine secrecy orders have become when law enforcement targets an American's email, text messages, or other sensitive data stored in the cloud. This abuse is not new. It is also not unique to one Administration and is not limited to investigations targeting the media and Congress.

Secrecy orders are too often used for routine investigations based on a cursory assertion that the government has met a statutory burden. The Justice Department's own template does not even require facts justifying the need for secrecy. Instead, the template merely asserts that any disclosure would seriously jeopardize the investigation for a variety of boilerplate reasons.

It's no surprise, then, that throughout the Obama, Trump, and Biden Administrations, up to a third of all legal demands we receive from Federal law enforcement include secrecy orders, up to 3,500 in just one year. These are just the demands on Microsoft. Add the demands likely served on Facebook, Apple, Google, Twitter, and others, and you get a frightening sense of the mountain of secrecy orders used by Federal law enforcement in recent years.

As has been pointed out, this is very different than investigations conducted before the advent of cloud computing. If law enforcement wanted to get access to data on a computer or a network in your home or your office, they would have to obtain and serve a warrant to enter your premise and collect evidence. If law enforcement wanted to secretly search your physical office, it had to meet the heightened standards required to get a so-called "sneak and peek" warrant. However, today, if law enforcement wants to secretly search your virtual office in the cloud, they just serve a boilerplate warrant and secrecy order on your cloud provider that prevents notice to you.

Microsoft scrutinizes each legal demand we receive to protect our customers' interests. We often challenge unnecessary secrecy orders through negotiation or litigation in court. Some examples, just examples, of some of the recent abuse we've seen are: Secrecy orders when the account holder was a victim, not a target, of the investigation; or when the investigation targets just one account at a reputable company, government, or university but the secrecy order bars notice to anyone in that organization; or where the government has secretly demanded records to evade an ongoing discovery dispute.

While Microsoft has long successfully challenged these secrecy orders in courts, litigation is no substitute for legislative reform. We worked with other technology companies and have reforms that we have proposed that permit secrecy orders for those rare cases where they are truly necessary.

We have four primary recommendations. First, Congress should end indefinite secrecy orders for good. We suggest that they last for 90 days, with a 90-day extension if proven necessary. Second, Congress must end rubber-stamp secrecy orders and require that judges engage in a written analysis of the relevant facts. Third, courts should apply strict scrutiny when issuing an order instead of only after it has been challenged. Finally, Congress should codify a statutory right authorizing cloud providers to challenge harmful secrecy orders to protect their users' rights.

Let me be clear, secrecy orders are sometimes necessary, such as to investigate cyber-attacks, to keep our children safe from online exploitation, or to prevent terrorist attacks. We don't suggest that the government must meet an impossible standard. We are asking for a meaningful one.

Notice to targets is an important safeguard for our constitutional rights. Reform is necessary to protect the fundamental values that are the bedrock of our democracy. Without reform, abuses will continue to occur, and they will occur in the dark.

Thank you for your time and attention.

[The statement of Mr. Burt follows:]

Written Testimony of Tom Burt
Corporate Vice President, Customer Security & Trust
Microsoft Corporation

United States House Committee on the Judiciary
Hearing on "Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power"

June 30, 2021

Chairman Nadler, Ranking Member Jordan, and Members of the Committee, my name is Tom Burt and I am the Corporate Vice President for Customer Security & Trust at the Microsoft Corporation. My team works to ensure customer trust in Microsoft's products and online services, and it includes our Law Enforcement and National Security team, which is responsible for responding to lawful access requests for customer data from governments around the world. I want to thank you for the opportunity today to provide Microsoft's perspective on the overuse of secrecy orders and the need for legislative reform.

The recent revelations that the Justice Department secretly targeted journalists and Members of Congress, their staff, and even their families with secret legal demands for their sensitive personal data were shocking to many Americans. But what may be most shocking is just how routine court-mandated secrecy has become when law enforcement targets Americans' emails, text messages, and other sensitive data stored in the cloud.

I want to be clear: The overuse and abuse of secrecy orders is not new, and in fact it has remained an ongoing problem since the ascendancy of cloud computing. It is not unique to one administration or political party. And it is certainly not limited to investigations targeting the media and Congress. Secrecy orders under 18 U.S.C. § 2705(b) — also known as non-disclosure orders — have unfortunately become commonplace. They are often approved even for routine investigations without any meaningful analysis of either the need for secrecy or the orders' compliance with fundamental constitutional rights.

Some may mistakenly assume that total secrecy is a standard feature of law enforcement investigations. But that has never been the case. Before the cloud, law enforcement agents executed search warrants and subpoenas seeking someone's personal correspondence and documents by serving them directly on the people or organizations they wished to search — in other words, the targets received notice. Law enforcement has historically functioned this way and done so with success.

In recent years, law enforcement has taken advantage of the efficiencies made possible because of the expansion of cloud computing and technology. As users have moved their email, photos and other data to the cloud, they should have the benefit of an increased expectation of privacy for that data as the cloud is much more secure than any internet connected computer in any home, business, or organization. But for citizens, businesses and organizations throughout America, this expectation of privacy is unknowingly misplaced. Their own government is secretly demanding users' data, without their knowledge, from cloud service providers, exploiting a subsection of the 35-year-old Electronic Communications Privacy Act to prevent notification of the demand to users by the cloud service providers. By doing so, the government has transformed decades-old criminal investigative techniques into secret surveillance operations — all without rigorous review by courts. This lack of transparency inevitably leads to overuse and abuse, such as the recently revealed subpoenas of data belonging to journalists and legislators.

Secret investigations: Once the exception, now a norm

Traditionally, secrecy was the exception. In recent years, law enforcement has turned that exception on its head, developing a practice of reflexively asking to keep even routine investigations secret. Providers, like Microsoft, regularly receive boilerplate secrecy orders unsupported by any meaningful legal or factual analysis.

While a few courts have criticized the government for submitting boilerplate applications,[1] there is significant evidence that courts do not regularly hold the government to any meaningful standard when determining, in secret ex parte hearings where only prosecutors are present, whether the requisite showing for secrecy has been made. Secrecy orders signed by judges typically include only a cursory assertion that the government has satisfied any or all of the statutory factors authorizing secrecy.[2] The Justice Department's own template for a surveillance order application under 18 U.S.C. § 2703(d) does not even require a prosecutor to provide facts justifying the need for secrecy. The template merely blindly asserts that any disclosure would "seriously jeopardize" the investigation for a variety of boilerplate reasons.[3]

It is no surprise, then, that such secrecy orders have become routine. At Microsoft, we are committed to transparency. Twice a year we release a public report that provides an extraordinarily close look at the legal demands we receive from law enforcement agencies around the world. We also fought in court for the right to publicly report on national security demands we receive each year — a right that this Committee helped to codify in the USA FREEDOM Act of 2015.

We have reviewed the number of secrecy orders that federal law enforcement agencies have presented to us from 2016 to the present, a period that spans the Obama, Trump, and Biden administrations. We found that while the number has increased some, federal law enforcement has consistently presented us with 2,400 to 3,500 secrecy orders each year, or 7-10 per day**,**

---

[1] "In each [of 15 separate applications seeking a secrecy order], the application relies on a boilerplate recitation of need that includes no particularized information about the underlying criminal investigation. For the reasons set forth below, I now deny each application without prejudice to renewal upon a more particularized showing of need. . . ." *In re Grand Jury Subp. Subp. to Facebook*, 2016 WL 9274455, at *1 (E.D.N.Y. May 12, 2016). *See also, e.g., In re Subp.*, 2018 WL 565004, at *2 (D. Nev. Jan. 25, 2018) ("The application as currently submitted fails to establish sufficient grounds for a non-disclosure order. First, a particularized showing of need has not been made and, instead, the application rests on boilerplate assertions that could be made with respect to essentially any grand jury proceeding.").

[2] Under 18 U.S.C. § 2705(b), a court shall enter a secrecy order if it determines there is reason to believe that notification of the underlying legal process will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

[3] The template states: "The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this [underlying surveillance] Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution." *See* "Sample 18 U.S.C. § 2703(d) Application and Order," Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009).

representing one-quarter to one-third of all the legal demands we received. These are just the demands that Microsoft, just one cloud service provider, received. Multiply those numbers by every technology company that holds or processes data, and you may get a sense of the scope of the government's overuse of secret surveillance.

The fact that law enforcement requested, and courts approved, clandestine surveillance of so many Americans represents a sea-change from historical norms. If law enforcement wants to secretly search someone's *physical* office, it must meet a heightened burden to obtain a sneak and peak warrant. More specifically, law enforcement has to prove to a judge with specific and articulable facts that a secret warrant is necessary and Congress placed a strict, presumptive 30-day limit on the length of time that secrecy may last. However, if they want to search your *virtual* office, they just serve a simple warrant on your cloud provider and obtain secrecy through a boilerplate process. Just a decade ago, in 2010, federal judges approved fewer than 2,400 requests for sneak and peak warrants nationwide[4] — a smaller amount than the number of secrecy orders that Microsoft alone received in any of the last five years.

Microsoft does not simply comply with such demands without question. We review them closely to protect our customers' interests. Some of the demands Microsoft received were legally deficient and we did not comply. In other cases, we have challenged — through negotiation or litigation — the orders. This includes secrecy orders approved by courts where the account holder was not a target of the investigation but a victim; where the investigation related to just one email account belonging to a large, reputable organization — a company, government, or school — and there was no allegation that the organization itself or its leadership was suspected of wrongdoing; where the government was engaged in discovery negotiations with an organization under investigation, and then secretly demanded the very same records from us to evade a dispute over privilege and the extent of discovery; and even where the owner of the target account consented to the search.

Our record challenging unnecessary secrecy

In fact, Microsoft has a long history of successfully challenging unnecessary secret surveillance, both directly in conversations with law enforcement and formally in court. Often, law enforcement will realize its secrecy demand lacks justification and will agree to let us provide advance notice to the owner of the target account. Sometimes law enforcement authorities even concede they came to us because it was simply "easier." Of course, "easier," is not, and should never be, the basis for a secrecy order.

When we cannot come to an arrangement with the government that allows us to provide advance notice, sometimes we challenge secrecy orders in court. In 2014, we sued the federal government to allow us to notify a customer who was targeted with a National Security Letter. The government eventually withdrew the demand and went to the customer directly for the information. In 2016, Microsoft brought a declaratory judgment action, asking a federal district

[4] Report of the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions, 2010, *available at* https://www.uscourts.gov/sites/default/files/2010_delayed_notice_search_warrant_report_0.pdf.

court to find that indefinite secrecy orders are unconstitutional. In response, the Justice Department issued guidance intended to limit secrecy orders to one year. In two cases unsealed just this year, the government relented to our requests and agreed to allow notice to our customers after we filed suits in court. And just last month, while preparing for oral argument in a case before the Second Circuit, the Justice Department asked the court to vacate another secrecy order we had challenged and to dismiss the case as moot. While our company has had success challenging secrecy orders in the courts, we have found that these individual challenges do not stem the tide of unnecessary secrecy orders. Litigation is no substitute for legislative reform.

Many of these orders should never have been approved by the courts. The current rubberstamping process places the onus on providers to challenge inappropriate secrecy orders. But providers have access to only the very limited information included in the secrecy order and underlying legal process, leaving providers in the dark about the supposed factual bases underlying the purported need for secrecy. We often have no idea, and no way to learn, whether the secrecy order is one of the very few that are truly justified, or not.

These problems are compounded for orders impacting consumer accounts. Consumer email addresses are generally anonymous. When Microsoft received one of the secret subpoenas that we now know targeted a congressional staffer in 2017, we were not aware of who the individual was or what the subpoena concerned. The laws and Justice Department policies did not require the government to provide us with any such information about the demand. It was only after the secrecy order expired and Microsoft – not the government – notified the individual about the subpoena that we learned about the troubling circumstances at issue.

A path forward

Thirty-five years ago this month, this very Committee held a markup and reported out the bill that governs secret electronic surveillance orders. The Electronic Communications Privacy Act became law at a time when only a tiny fraction of Americans had personal computers. We were still years away from a rudimentary at-home internet. Congress simply could not have envisioned modern cloud computing, or how our most basic and fundamental concepts of privacy have become wholly dependent on the security of our data in the cloud.

It's time for this Committee to update this antiquated law. The time is right to reform secrecy orders to prevent their overuse and abuse. Only a few key changes are necessary to protect the rights of Americans from unwarranted secret surveillance.

The reform principles we are proposing would not prevent secrecy when truly necessary to protect an investigation. Rather, they would require judges to carefully consider, based on an individualized factual showing, whether to approve a secrecy order. These reforms would bring the statute in line with how searches are conducted in the physical world. They would bring the statute in line with the Constitution. And they would expand on important secrecy order reforms contained in prior, broader ECPA reform efforts that Microsoft has supported for years.

First, Congress should end indefinite secrecy orders for good. One of Microsoft's lawsuits resulted in a new Justice Department policy in 2017 that was intended to limit secrecy orders to one year; unfortunately, we continue to receive federal orders approved with no expiration date at all. We suggest that secrecy orders be limited to a reasonable time, such as 90 days, with extensions of the same length available when the continued need for secrecy is justified based on articulated facts and approved by a judge.

Second, we believe the government should be required to provide notice to the target of a demand for data upon the expiration of a secrecy order. While Microsoft makes these notifications now, it is unclear whether all providers follow the same practice. Moreover, ensuring the fundamental right to know when a person's virtual office or virtual data has been searched should not be left to the vagaries of companies' preferences and processes, but should occur uniformly by the very government who executed the covert search.

Third, Congress must make the standard to obtain a secrecy order meaningful. To address the trend of boilerplate motions and orders, we suggest that courts be required to find, based on specific and articulable facts and documented in their written findings, that one of the current statutory factors for secrecy is likely met, replacing the statute's current nebulous "reason to believe" standard. Simply requiring a full, meaningful, reviewable written analysis will have an enormous impact on the decision making of both the Justice Department and the courts.

Fourth, the standard for a secrecy order must also be made consistent with the First Amendment. Courts have rightly held that a secrecy order is a government mandate that a provider refrain from exercising its freedom of speech, and that providers can challenge secrecy orders under the First Amendment.[5] But courts have not traditionally applied the First Amendment strict scrutiny standard when *issuing* the secrecy order; they have applied this standard only when considering a challenge after the fact, approving countless orders without any meaningful First Amendment review. We suggest that Congress close this constitutional loophole by requiring courts to find, before approving a secrecy order, that the order is narrowly tailored to achieve a compelling government interest, consistent with the First Amendment.

Fifth, providers have seen too many examples of the government preventing notification of a demand to a large organization or university when only one employee or student's email account is being searched, and when the organization is not suspected of any wrongdoing. This appears to be what happened to Google with *The New York Times* investigation. Before cloud computing, these organizations would have received court orders directly, and there is simply no justification to keep them in the dark just because they use the cloud. Google rightly pushed back, and we do, too. But providers should not be the only ones standing up for the constitutional rights of those impacted by government surveillance. When approving an order, courts should find that no one representing the company, school, or other organization on whose domain the data is hosted could be notified without an adverse result under the statute occurring. Simply requiring a judge to ask that question will prevent numerous inexcusably overbroad secrecy orders.

[5] *See, e.g., Microsoft Corp. v. United States Dep't of Justice*, 233 F. Supp. 3d 887, 900 (W.D. Wash. 2017); see also *Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Cal. 2017).

Sixth, we need more transparency around secrecy orders, both in terms of their overall use and the information providers and users can access to allow them to properly consider their rights when confronted with an order.

Finally, despite the undeniable impact of secrecy orders on the rights of both providers and our customers, some courts have found that providers lack standing to challenge such orders. We suggest that Congress codify a statutory right to allow providers to intervene to challenge harmful secrecy orders, to protect their users and to ensure the statutory and constitutional requirements are met.

These reforms, taken together, would serve as a strong foundation for ending the abuses of secrecy orders that Microsoft and other technology providers see each day. At the same time, it would enable the issuance of properly narrow, time limited and factually justified secrecy orders when truly necessary to protect a criminal investigation.

In closing

Before I close, I also want to reiterate that we do not oppose all secrecy orders. We cooperate with the Justice Department to investigate criminal and national security cyber-attacks, to keep our children safe from online exploitation, to disrupt criminal enterprises, and to prevent terrorist attacks. In fact, through our Digital Crimes Unit we actively work, together with law enforcement, to deter or prevent such crime. Certain sensitive investigations merit non-disclosure orders. We are not suggesting that secrecy orders should only be obtained through some impossible standard. We simply ask that it be a meaningful one.

Government accountability depends on transparency. That concept is central to our democracy. Secrecy should be the rare exception, not the norm. Providing notice to an individual the government targets with a warrant or other demand for information is a critical protection against government overreach. Safeguarding one's constitutional rights requires knowledge that those rights are at risk. Without notice, an individual is left in the dark, unable to raise privileges or other objections that may be applicable, and unable to protect their rights in court. Reform is necessary to protect the reasonable privacy expectations and rights of the press, our legislators, their staff and their families. It is needed to protect all of Microsoft's customers and the customers of other cloud service providers. It is needed to protect fundamental values that are the bedrock of our democracy.

Through our advocacy here in Congress, in the courts, and with law enforcement, Microsoft will continue to do everything it can to prevent the misuse of secrecy orders. But we respectfully request that you work with us to fully address this problem. Without legislative reform, abuses will continue to occur — and they will continue to occur out of sight.

Thank you for your time and attention.

# # # # #

Chair NADLER. Thank you for your testimony.
Professor Turley, you may begin.

TESTIMONY OF JONATHAN TURLEY

Mr. TURLEY. Thank you, Mr. Chair, Ranking Member Jordan, Members of the Judiciary Committee. Thank you for inviting me to speak today.

The reported targeting of reporters and Members of Congress in the recent leak investigation is a serious matter that cuts across areas of constitutional and statutory law. It should also cut across partisan lines to unify the public and the Congress in seeking answers to these difficult and troubling questions.

Today's hearing occurs on the 50th anniversary of *The New York Times*' publication the Pentagon Papers, an act that triggered one of the most consequential legal battles in the history of this country, a battle that ultimately helped define the rights of the free press.

It also reminds us that drawing the line between national security and press freedom continues to evade clear demarcation. Indeed, it was 15 years ago that I testified before the House Intelligence Committee and called again for the enactment of a Federal shield law. It's a reminder of how this area remains dangerously ill-defined and uncertain for reporters, particularly with the growth of new technology that has made a mockery of many of our protections.

This is a difficult area because there's compelling arguments on both sides, by the Department of Justice and by the media, and courts have struggled with what is often presented as a zero-sum game. You can see that in the cases that I discuss in my testimony.

So, this is a very serious matter. We don't know all the facts, but it cuts across and raises issues of separation of powers, the free press, and privacy. I would like to, however, focus on where I ended 15 years ago, and that is on the necessity of a Federal shield law. I will note that my testimony identifies six areas that I believe should be explored in light of this controversy.

Frankly, for those of us who have advocated for the free press and for free speech, this is what Yogi Berra meant when it was all "déjà vu all over again." We have seen this in the Bush Administration, we've seen it in the Obama Administration, we've seen it in the Trump Administration, we saw it at the beginning of the Biden Administration. It's foolish to believe that anything is going to change. In fact, that, I believe, is the definition of "insanity"—of doing the same thing, expecting a different result.

The fact is, we rely uncomfortably on self-regulation by the Department of Justice. They have not met that burden. They have failed over and over again.

It is not partisan. It cuts across parties and Administrations. It is a record of failure that puts at risk one of the most precious rights, one of the most essential rights in our constitutional system, and that is the free press.

The six areas I laid out include concerns over the authorization in this matter, what I call "reverse engineering" of leak investigations, gag orders, fishing in the cloud, which is a major problem, national security letters, and defining "journalism."

I really would like this Committee to begin and end—and this will come as no surprise to the Chair and the Ranking Member, that I invoke James Madison. As a Madisonian scholar, I think most things begin and end with James Madison. Madison said most famously, "A popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy or perhaps both. Knowledge will forever govern ignorance, and people who mean to be their own governors must arm themselves with the power that knowledge gives." It's the free press that gives us that knowledge. It's the free press that protects us most certainly from tyranny.

I won't address the case law that I have discussed, but I will note this: The State legislatures have been for more protective of the free press than this body. There are 16 States and the District of Columbia that have absolute privileges for the media. There are 24 States that have qualified privileges for the media. Other States that don't have those shield laws actually have common-law protections for the media.

The Free Flow of Information Act of 2017 is a great platform. It is supported by both parties, and it is time that we move that to enactment. I am critical of aspects of the law, even though I would take that law right now in a heartbeat to try to gain that protection for the media. I note that it could be strengthened with a greater explanation of presumptions. Also, I believe it has to be rewritten on the definition of what constitutes a journalist. Journalism has changed in this world, and the definition in the law is frozen in journalistic amber that is ages out of date. So, I would suggest examining that.

I will only end with this, as I did 15 years ago: We cannot afford the consequences of leaving the media exposed the way we have. That will leave not just them exposed but the public in the dark. It will be, as Madison said, "a prologue to a farce or a tragedy or both." We can avoid both, and we need to pass this law.

Thank you.

[The statement of Mr. Turley follows:]

Statement for the Record
Jonathan Turley
J.B. and Maurice C. Shapiro Professor of Public Interest Law
George Washington University Law School

"Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power"

Before the Committee of the Judiciary

June 30, 2021

I. INTRODUCTION

Chairman Nadler, Ranking Member Jordan, members of the Judiciary Committee, thank you for inviting me to testify on secrecy orders and the investigation of unauthorized disclosure of classified information. The reported targeting of reporters and members of Congress in recent leak investigations is a serious matter that cuts quite broadly across areas of constitutional and statutory law. It should also cut across any partisan lines to unify the public and the Congress in seeking answers to these difficult and troubling questions. The subject of today's hearing carries particular significance for me as someone who has litigated,[1] testified,[2] taught,[3] and written in

---

[1] My past national security cases range from terrorism cases to espionage cases to classified environmental cases. These cases include the Area 51 litigation, the defense of Dr. Ali Al-Timimi, the defense of Dr. Sami Al-Arian, the defense of Harold James ("Jim") Nicholson, the defense of Petty Officer Danny King, and Dr. Thomas Butler. I have also represented the United States House of Representatives in court as well as a House Intelligence officer accused of national security violations. I have also advised the legal team of Julian Assange on United States criminal and national security issues as part of his extradition proceedings in London.

[2] I have previously testified in Congress as both a Democratic and Republican witness on a variety constitutional and statutory issues, including national security, oversight, and free press issues. *See, e.g.*, United States House of Representatives, Committee on the Judiciary, *Executive Privilege and Congressional Oversight*, May 15, 2019; United States House of Representatives, House Committee on Science, Space, and Technology, *Affirming Congress' Constitutional Oversight Responsibilities: Subpoena Authority and Recourse for Failure to Comply with Lawfully Issued Subpoenas*, September 14, 2016; United States House of Representatives, Committee on the Judiciary, *The President's Constitutional Duty to Faithfully Execute the Laws*, December 2, 2013; United States House of Representatives, Committee on the Judiciary, *Reckless Justice: Did the Saturday Night Raid of Congress Trample the Constitution*, May 30, 2006; United States House of Representatives, Permanent Select Committee on Intelligence, *The Media and The Publication of Classified Information*, May 26, 2006; United States House of Representatives, Subcommittee on Homeland Security, *Protection of Privacy in the DHS Intelligence Enterprise*, April 6, 2006; United States House of Representatives, House Judiciary Committee, *The Constitutionality of NSA Domestic Surveillance Operation*, January 20, 2006; United States Senate, Senate Judiciary Committee, Subcommittee on Terrorism, Technology, and Homeland Security, September 13, 2004; United States Senate, Select Committee on Intelligence (closed classified hearing), *The Prosecution and Investigation of the King Espionage Case*, April 3, 2001.

[3] As an academic, I teach and write in the areas of constitutional law, privacy, and constitutional criminal procedure.

the areas of national security and privacy law for over thirty years.[4] I have also worked in the media as a columnist and legal analyst for roughly three decades.[5]

Today's hearing occurs on the 50th anniversary of the New York Times' publication of the Pentagon Papers story—triggering what would become one of the most consequential legal battles in our history on the meaning of the free press under the First Amendment. It also reflects how drawing a line between national security and press freedom continues to evade clear demarcation. Indeed, it was fifteen years ago that I testified before the House Intelligence Committee[6] on these issues and the area remains just as dangerously ill-defined and uncertain, if not more so due to new technological realities. What makes the question even more challenging is that both sides have compelling arguments and legitimate interests to advance. Despite being an outspoken advocate for free speech and the free press throughout my career, I have always recognized that the government has a legitimate interest in conducting leak investigations. This can create the ultimate example of the immovable object (of the media) confronting the irresistible force (of the government). Courts have struggled to resolve the zero-sum nature of this conflict. They have long recognized the legitimacy of leak investigations in the interest of national security. In *Haig v. Agee*, for example, the Court stressed that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[7] Yet, the courts also recognize that such national security laws cannot be allowed to curtail free speech or free press rights as guaranteed by the Constitution.[8] As the Court stated *Bartnicki v. Vopper*, "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[9]

I would like to begin where I ended fifteen years ago on the need for a federal shield law for the media. There remains a great deal that is not known about the recently disclosed subpoenas issued in February 2018 under the Trump Administration with regard to Apple iCloud accounts.

---

[4] These publications include *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 Boston University Law Review 2179 (2020); *Through a Looking Glass Darkly: National Security and Statutory Interpretation*, 53 Southern Methodist University Law Review 205-249 (2000) (Symposium); *The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court*, 79 Journal of Criminal Law and Criminology 66-134 (1988).

[5] I have previously worked as a legal analyst for NBC/MSNBC (twice), CBS (twice), and BBC. This year I left CBS and BBC to work as Fox legal analyst. I also write as a columnist for USA Today and The Hill as well as periodic columns in other national newspapers. Finally, I am the host of Res Ipsa (www.jonathanturley.org), a legal and policy blog. The views expressed today are entirely my own and not those of my school or my associated media companies. That includes my sole responsibility for any typos or errors in this rushed testimony despite the inspired proofing of my colleague Thomas Huff and my assistant Seth Tate.

[6] United States House of Representatives, Permanent Select Committee on Intelligence, *The Media and The Publication of Classified Information*, May 26, 2006 (Professor Jonathan Turley).

[7] 453 U.S. 280 (1981) (citing Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964).

[8] *Mills v. Alabama*, 384 U.S. 214, 218 (1966); *see also United States v. Morison*, 844 F.2d 1057, 1086 (4th Cir. 1988) (Phillips, J., concurring) ("notwithstanding information may have been classified, the government must still be required to prove that it was in fact 'potentially damaging ... or useful,' *i.e.*, that the fact of classification is merely probative, not conclusive, on that issue, though it must be conclusive on the question of authority to possess or receive the information. This must be so to avoid converting the Espionage Act into the simple Government Secrets Act which Congress has refused to enact.").

[9] 532 U.S. 514, 527 (2001).

It appears that "metadata"[10] or other information may have been sought on various individuals associated with the House Intelligence Committee, including most notably Democratic ranking member Adam Schiff and Rep. Eric. Swalwell. If true, this is an extremely serious matter with implications for the separation of powers, the free press, and privacy. As a Madisonian scholar, I admittedly favor the legislative branch in many disputes with the executive branch. However, such demands would give pause to even the most ardent advocates of executive power.[11] These searches also reportedly included media targets and were accompanied by gag orders preventing the disclosure of the demands to customers. We have much to learn about these demands but the one thing that should be clear is that we need a federal shield law as well as other measures to address new threats to both media and privacy interests.

II.
GENERAL OBSERVATIONS ON THE CURRENT CONTROVERSY

For those of us who support robust protections for the press, the current scandal is what Yogi Berra would call "deja vu all over again." After the Watergate and Pentagon Paper scandals, the public demanded protections for the media and whistleblowers. However, each scandal was met by legislative responses that failed to protect the media from abusive searches. Guidelines are only as good as they are enforceable, including the use of adversarial processes. For example, the current guidelines mandate that searches and subpoenas targeting reporters must be "extraordinary measures, not standard investigatory practices."[12] However, while we still need more details on these demands, the current controversy would suggest the same pattern of the casual targeting of media sources. Much of our current system relies on the self-regulation by the government, which has repeatedly failed that test. There remains a need for greater judicial review and transparency. As Judge Tatel noted in *In re Grand Jury, Judith Miller*, the Executive Branch "possesses no special expertise that would justify judicial deference to prosecutors' judgments about the relative magnitude of First Amendment interests. Assessing those interests traditionally falls within the competence of courts."[13] The alternative is to repeat the regular pattern of abuses, apologies, and assurances from the Justice Department.

During the Bush Administration, New York Times reporters Eric Lichtblau and James Risen were targeted by secret searches after they co-authored an article on the Bush Administration NSA's warrantless surveillance program. The belated disclosure of the searches was followed by

---

[10] Metadata is generally defined "data about data" and includes vital identifiers and descriptors on communications. Such metadata is often needed for searches of vast bodies of electronic data to isolate and organize sources. It often reveals information about when the document was created or last modified, and its history and author. *See generally* Ben Minegar, *Forging a Balanced Presumption in Favor of Metadata Disclosure Under the Freedom of Information Act*, 16 J. Tech. L. & Pol'y 23, 24 (2015).

[11] This point was made previously by former Vice President Mike Pence when a member of the House in support of a federal shield law. He declared "[a]s a conservative who believes in limited Government, I know that the only check on Government power in real-time is a free and independent press. The 'Free Flow of Information Act' is not about protecting reporters. It is about protecting the public's right to know." Free Flow of Information Act of 2007: Hearing Before the H. Comm. on the Jud., 110th Cong. 32-34 (June 14, 2007) (Rep. Mike Pence).

[12] 28 C.F.R. § 50.10(a)(3).

[13] 438 F.3d 1141, 1175-76 (D.C. Cir. 2006).

the same perfunctory apology from the FBI and the promise for future steps to protect the media.[14]

During the Obama administration, the Justice Department under then Attorney General Eric Holder ordered a full investigation targeting then Fox News reporter James Rosen. Rosen was investigated for simply speaking with a source in a story involving classified information. Even the phone numbers of Rosen's parents were not spared in an operation that was said to have been approved by Holder. More than 20 lines linked to Associated Press reporters were also secretly targeted. The Justice Department evaded its own policies by branding Rosen a "co-conspirator" in the crime of information leakage.[15] The scandal was followed by apologies, policy changes,[16] and pledges that the media would be protected in the future.[17]

During the Trump Administration it was revealed that the Justice Department seized the phone and email records of New York Times reporter Ali Watkins as part of an investigation of a legislative aide.[18] It has now been alleged that, during the Trump Administration and the early Biden Administration, both media and members of Congress may have been targeted by secret searches. This controversy was followed by a meeting of media figures with Attorney General Merritt Garland, who offered the same apologies and reassurances of future reforms.

While I will focus on the constitutional issues and the need for a shield law, I would like to briefly raise six concerns about the current controversy. As I stated when this operation was first disclosed,[19] the accounts of this investigation raise serious concerns about the conduct of the Justice Department.

1. Authorization. It is notable that former Attorneys General Jeff Sessions and Bill Barr as well as Attorney General Merrick Garland all deny knowledge of the investigation in the Trump and Biden Administrations. That should not be the case under current federal policies and regulations. Since the 1970s, the Justice Department has required such authorization.[20] This requirement for approval by the Attorney General or a designated high-ranking official was reaffirmed after a scandal in the Obama Administration.[21] The Justice Department agreed to the protection "[b]ecause freedom of the press can be no broader than the freedom of members of the

---

[14] *F.B.I Says it Obtained Reporters' Phone Records*, N.Y. Times, Aug. 8, 2008.

[15] Application for Search Warrant dated May 28, 2010 & Aff. of Reginald Reyes in Support, *USA v. Email Account Redacted@Gmail.com*, No. 1:10-mj-00291 (D.C. Cir., unsealed Nov. 7, 2011) (Dkt. Nos. 20 & 20-1).

[16] DOJ Report on Review of News Media Policies (July 12, 2013).

[17] Charlie Savage, *Holder Tightens Rules on Getting Reporters' Data*, N.Y. Times, Jul. 7, 2013.

[18] Adam Goldman, et al., Ex-Senate Aide Charged in Leak Case Where Times Reporter's Records Were Seized, N.Y. Times (June 7, 2018), available at https://www.nytimes.com/2018/06/07/us/politics/timesreporter-phone-records-seized.html.

[19] Jonathan Turley, *If You Want To Protect Journalists, You First Need To Define Them*, USA Today, June 13, 2021, available at: https://jonathanturley.org/2021/06/16/the-leak-investigation-if-we-want-to-protect-journalists-we-first-need-to-define-them/

[20] 28 C.F.R. § 50.10(a)(1) (2005).

[21] Off. of the Attorney Gen., *Updated Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media* (Jan. 14, 2015), https://www.justice.gov/file/317831/download; DOJ Justice Manual § 9-13.400 (updated Jan. 2020), https://www.justice.gov/usam/usam-9-13000-obtaining-evidence#9-13.400.

news media to investigate and report the news, the Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering activities."[22] Any investigation of a member of Congress or the media should not occur without the highest knowledge and approval. If the three Attorneys General were not fully briefed on this operation, it is a very serious failure of the system and should not go unaddressed by this body.

2. Reverse Engineering. My greatest concern is whether the Justice Department has continued to "reverse engineer" such investigations. The problem is not that an investigation into the leaks confirmed telephone numbers or addressed related to journalists. Such contact information is part of any leak investigation. Moreover, there was ample reason for investigation. The Trump Administration was hit with an unprecedented number of leaks. Some of those leaks appeared to occur in astonishingly short periods of time after conversations in the White House, including with the President. As a result, the Administration publicly announced that it would pursue such leaks aggressively. Few people dispute that the federal government has a legitimate interest, if not an obligation, to investigate the unauthorized of classified or sensitive information. These leaks are criminal acts under federal law. The real concern is whether the investigation targeted the recipients of these leaks, rather than the leakers themselves. Prosecutors and investigators are often tempted to reverse engineer a leak, starting with the recipients of the information and working back to identify the senders. The government often knows the recipients of classified information just by looking at the byline on the articles. It is much easier for the investigation but it is also much more damaging for the Constitution.

The issue is not that the government should be barred from confirming numbers of journalists as part of leak investigations. Such investigations are important not just to protect national security but privacy and other rights. Indeed, a president cannot effectively operate if denied confidentiality of communications with staff or foreign leaders. While Congress is (rightly) demanding answers on the targeting of its members and journalists, many are also calling for an investigation into the leaks after the tax record of select billionaires were released.[23] The leak of these tax records is a federal crime and appears likely to have originated from a hack of IRS records or an actual IRS employee or contractor. If the Justice Department finds a suspect, tracing that person's calls or data may reveal contacts in the media, public interest groups, and other associations. The Pro Publica article was a classic use of a leak. If this was an IRS employee, it was someone who believed they were acting in the public interest as a whistleblower. It was also someone who was committing a federal crime. Regardless of the source of the tax information, the one thing the Justice Department should not do is reverse engineer its investigation by targeting Pro Publica staff. When the media relied on the Edward Snowden leaks, it was done to denounce the unconstitutional surveillance of citizens during the Obama administration. This has brought about substantial and needed changes. However, no one has sought to prosecute the New York Times reporters or editors. Conversely, few have questioned the legitimate effort to arrest Snowden as responsible for the leak. The Justice Department should seek to find the leaker, but it should do so by targeting those suspected of disclosing the information rather than reporters who received it.

---

[22] *Id.*

[23] Jesse Eisinger, Jeff Ernsthausen & Paul Kiel, *The Secret IRS Files; Trove of Never-Before-Seen Records Reveal How The Wealthiest Avoid Income Tax*, Pro Publica, June 8, 2021.

3. Gag Orders. The reported imposition of a gag order on these companies magnifies the concerns over the protection of the free press and privacy. There is a growing need for legislative and policy changes on such gag orders. In the secret orders targeting CNN's Pentagon reporter Barbara Starr in 2017, the Justice Department reportedly fought to maintain a gag order that ultimately was found to be too broad and sweeping. Such orders can magnify abuses. It allows the government to not only conduct secret searches with little required showings but also allows the government to then prevent others from challenging its actions to halt possible abuses.[24]

These orders are troubling on a variety of levels. They not only make these companies effective agents of the government but they require them to effectively deceive their clients who continue to share information under the assumption that these are private communications. Court orders often limit who corporate officials can consult as they seek to challenge the limitations. It is easy to see the utility for the government in hiding such searches from possible targets. Yet, the authority to do so has long been controversial. These companies are not targets or suspects or knowing abettors. However, they are being forced into silence—often on the mere suspicion of unlawful conduct of third parties. These companies could have principled objections to cooperating on some searches or the means being used by the government. Notably, some courts have found that even people warning drivers of speed traps are protected under the Constitution.[25] However, if a company warns a customer of a search, it is deemed in violation under these orders. Again, there are good-faith interests on both sides but there has been little debate over the use and basis of such authority in Congress. At a minimum, the use of such gag orders should be narrowly defined, sharply curtailed, and carefully monitored.

4. Fishing in the Cloud. The current controversy highlights the vulnerability of data held in "the Cloud." While the government is required to satisfy probable cause for searches of computers, it has been able to circumvent that Fourth Amendment protection in acquiring electronic data under a minimal reasonable suspicion standard. (As discussed below, the growth of these searches followed court decisions limiting the need for warrants). This can be accomplished under the Stored Communications Act of Title II of the Electronic Communications Privacy Act of 1986. Agents need to "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[26] It is important to note that any media leak investigation will easily satisfy that standard since the disclosure of classified or privileged information is confirmed in the publication itself. The storage of such information represents the type of technological leap that has regularly undermined constitutional protections.[27] The fact that information is stored on the Cloud should

---

[24] This includes the use of boilerplate claims to nondisclosure orders. *In re Grand Jury Subp. Subp. to Facebook*, 2016 WL 9274455, at *1 (E.D.N.Y. May 12, 2016) ("In each [of 15 separate applications seeking a secrecy order], the application relies on a boilerplate recitation of need that includes no particularized information about the underlying criminal investigation. For the reasons set forth below, I now deny each application without prejudice to renewal upon a more particularized showing of need.").

[25] *See*, *e.g.*, *Florida Court Rules That Flashing Lights To Warn Other Drivers of Speed Trap is Protected Speech*, Res Ipsa, May 23, 2012, available at https://jonathanturley.org/2012/05/23/florida-court-rules-that-flashing-lights-to-warn-other-drivers-of-speed-trap-is-protected-speech/

[26] 18 U.S.C. § 2703(d).

[27] Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 Boston University Law Review 2179 (2020).

not be material to the privacy protections afforded that information. Moreover, the Stored Communication Act allows for a nondisclosure order but has no limit on its duration for a court.[28]

5. National Security Letters. Civil libertarians have long objected to the use of National Security Letters (NSLs), which have historically been abused by the federal government, including violations of the underlying statutes and the use of "exigent letters" (rather than formal NSL submissions). NSLs seek transactional information in national security investigations from communications providers, financial institutions, and credit agencies.[29] When Congress enacted the Right to Financial Privacy Act (RFPA), it made an exception to specify that "Nothing in this chapter . . . shall apply to the production and disclosure of financial records pursuant to requests from—(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities; [or] (B) the Secret Service for the purpose of conducting its protective functions."[30] This was not an authorization for mandatory NSLs. Indeed, Congress assumed that companies could refuse such letters.[31] However, Congress passed incremental amendments expanding the authority for NSLs. These expansions, particularly after the Patriot Act, raised concerns under both the First Amendment and the Fourth Amendment.[32] Later Congress enhanced this authority further with judicial enforcement provisions in the 109th Congress.[33] With the ever-expanding authority given to agencies, NSLs have surged. From 2000 to 2005, for example, NSLs grew from 8,500 to 47,000.[34] The reason is obvious. Such demands require little showing from the government and evade the conventional warrant process under the Fourth Amendment.

What is particularly chilling is that NSLs are often used under this lower standard to satisfy the applications for secret searches in the Foreign Intelligence Surveillance Act (FISA) court.[35] Inspector general investigations have found extensive abuses in recent years in the use of NSLs. Both NSLs and FISA searches operate below the traditional probable cause standard and, again not surprisingly, they have ballooned as the search avenues of choice for investigators.

The abuse of NSLs is a problem created not just by Congress but the courts. The Supreme Court ruled in 1979 in *Smith v. Maryland*[36] that there was no expectation of privacy in telephone numbers given to telephone companies as a third party. Thus, pen registers are not treated as

---

[28] 18 U.S.C. § 2705(b).

[29] *See generally* Congressional Research Service, *National Security Letters in Foreign Intelligence Investigations*, July 30, 2015.

[30] Section 1114, P.L. 95-630, 92 Stat. 3706 (1978); now codified at 12 U.S.C. 3414(a)(1) (A), (B).

[31] CRS, supra, at 1 ("It was neither an affirmative grant of authority to request information nor a command to financial institutions to provided information when asked.").

[32] See, e.g., *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 876-77 (2d Cir. 2008), *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004), *vac'd and remanded*, 449 F.3d 415 (2d Cir. 2006). *See also In re National Security Letter*, 930 F.Supp.2d 1064, 1081 (N.D.Cal. 2013) ("[T]he Court concludes that the nondisclosure provision of 18 U.S.C. §2709(c) violates the First Amendment and 18 U.S.C. §3511(b)(2) and (b)(3) violate the Frist Amendment and separation of powers principles").

[33] 28 U.S.C. 3511.

[34] U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 120 (March 2007).

[35] CRS, supra, at 6.

[36] 442 U.S. 735, 745 (1979).

searches under the Fourth Amendment's probable cause requirement. With the expansion of new technology on data storage and transfer, more data is being sucked into this vortex of unprotected or less protected material or communications. At the same time, there is a growing disconnect with other more protected areas. For example, the Court ruled in *Carpenter v. United States*[37] that it is a violation of the Fourth Amendment to track the location of cell phones without a warrant. Many of us celebrated that ruling. There is an obvious inconsistency with the requirement that the government obtain a warrant to obtain locational information from cellphone companies but no such warrant requirement for obtaining metadata revealing contacts and communication information.

The problem in these cases was highlighted in *New York Times v. Gonzales*.[38] The Second Circuit was faced with a refusal of the New York Times to grant access to its phone records as part of a terrorist investigation. The government indicated that it would seek the records directly from a third-party cloud service provider and that provider refused to inform the newspaper if it was compelled to release the information. The Justice Department denied that it has "an obligation to afford The New York Times an opportunity to challenge the obtaining of telephone records from a third party prior to its review of the records, especially in investigations in which the entity whose records are being subpoenaed chooses not to cooperate with the investigation."[39] The court found that the constitutional concerns did not warrant intervention in the case. However, as Judge Sack stated in his dissenting opinion, the question is "not whether the plaintiff is protected in these circumstances, or what the government must demonstrate to overcome that protection, but to whom the demonstration must be made."[40] As with the lack of protections for journalists by the Court discussed below, this is an area that will likely require congressional action if we are to protect privacy and speech interests. That includes bolstering appeals, adversarial proceedings, and standing to guarantee greater judicial review.

6. Defining Journalism. Finally, it is worth noting that any effort to protect the media will return Congress to a question that has been left unanswered by design, or at least by general resignation: what is a journalist? It is generally accepted that the tax disclosure was a case of investigative journalism. After all, Pro Publica has won six Pulitzer Prizes and stands as a nonprofit investigative group committed to exposing "abuse of power and betrayals of public trust by government, business and other institutions, using the moral force of investigative journalism to spur reform through the sustained exposure of wrongdoing." That sounds a bit familiar. WikiLeaks was founded as a non-profit organization "to bring important news and information to the public . . . to publish original sources alongside our reporting so that readers and historians can see evidence for the truth." In 2013, WikiLeaks was declared by the International Federation of Journalists as a "new generation of media organizations" that "provide important opportunities for media organizations" through the publication of such non-public information. Yet, the Justice Department is still fighting to extradite Assange. It uses the same tactics used in the Rosen case by treating Assange not as a journalist but as a criminal co-conspirator. The DOJ insists that Assange played an active role in his correspondence and advice with the hacker. Still, Assange would not be the first journalist to work with a whistleblower who

---

37 138 S. Ct. 2206 (2018).
38 459 F.3d 160 (2nd Cir., 2006).
39 *Id.* at 165.
40 *Id.* at 176.

prospectively acquires or continues to acquire non-public information. That is why a shield law is meaningless if the protected class is ill-defined.[41] I will discuss this issue further below.

We obviously need to learn much more about what occurred in this investigation and the ongoing Inspector General investigation will be critical in laying the foundation for any legislative reform. However, there is no reason why we cannot move forward on the long-needed passage of a federal shield law.

III.
THE "CHOICEST PRIVILEGE": THE ROLE AND PROTECTION OF THE FREE PRESS IN OUR CONSTITUTIONAL SYSTEM

As will come as little surprise to people who know me, I believe that any discussion of this latest controversy should start (and ideally end) with James Madison. The father of our Constitution made clear the central importance of a free speech in preserving the other rights guaranteed under the Bill of Rights. He wrote in one of his most cited passages:

> "[a] popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance. And a people who mean to be their own Governors must arm themselves with the power which knowledge gives."

It is a common lament that, as civil libertarians, we often must defend abstractions like free speech or the free press against concrete and immediate dangers often raised by the government. However, Madison articulated the reason for refusing a Faustian bargain in the limitation of the free press. It is not just that this is the "power which knowledge gives" but this is the very source of information that allows a free people to protect against tyranny. It is the guarantee, like free speech, that helps to guarantee the protection of other rights.

The Framers themselves could not be clearer. The First Amendment of the Constitution reads in relevant part, "Congress shall make no law . . . abridging the freedom of speech, or of the press."[42] Justice Hugo Black famously stated "I read 'no law abridging' to mean no law abridging."[43] For some of us, the importance of this quote is not to suggest an absolutism in the protection of free speech and free press (though I confess to supporting few limitations on these rights). It is to reaffirm that the natural default position under our Constitution should be the protection of both rights with a heavy presumption against encroachments from the government.

That natural default was evident in the words of key figures like Madison who referred to the "inviolable" right of the free press as the "choicest privileges of the people."[44] Madison was not

---

[41] Jonathan Turley, *The Assange Case Could Prove The Most Important Press Case in 300 Years*, BBC, available at https://jonathanturley.org/2019/05/26/the-assange-case-could-prove-the-most-important-press-case-in-300-years/

[42] U.S. CONST. amend. I.

[43] *Smith v. California*, 361 U.S. 147, 157 (1959) (Black, J., concurring).

[44] Jeffery A. Smith, PRINTERS AND PRESS FREEDOM: THE IDEOLOGY OF EARLY AMERICAN JOURNALISM 166 (1988) (quoting Letter from James Madison to Edmund Randolph (May 31, 1789), *in* 5 THE WRITINGS OF JAMES MADISON 372, 377, 380 (Gaillard Hunt ed., 1904)).

just speaking of prior restraints but the penalties that might be imposed for the exercise of this right. He noted that the American notion of the free press would extend beyond that of England. It was a telling observation since figures like William Blackstone defined the right as a protection against prior restraint.[45] Yet, Madison wrote "the essential difference between the British government and the American constitutions will place this subject in the clearest light."[46] That was evident in Madison's opposition to the Sedition Act of 1798. Madison observed that "it would seem to be a mockery to say that no laws should be passed preventing publications from being made, but that laws might be passed for punishing them should they be made."[47]

Obviously, this right is not absolute. The media can be sued for defamation and generally cannot commit crimes in the name of journalism. However, even on defamation, the Supreme Court has adopted a protective standard to protect the media from liability in *New York Times v. Sullivan*.[48] In both the freedom of speech and the free press, the Court has recognized the need for "breathing space" for these rights to play their desired role. The harm often claimed by the exercise of these rights is often a thinly veiled attack on the very essence of those rights.[49]

The protections afforded to the press have been curtailed through years of equivocating and distinguishing decisions. For the government in the national security area, the natural default often appears as not just deference but sweeping deference, even when targeting journalists. That is the position repeatedly advanced by the Justice Department in cases going back to the Pentagon papers controversy. Yet, the Court rejected sweeping arguments by the Justice Department in *New York Times Co. v. United States*.[50] The Court captured the rivaling interests. In his concurrence, Justice Stewart noted that "the frequent need for absolute secrecy is, of course, self-evident."[51] Conversely, Justice Douglas noted that "Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion issues are vital to our national health."[52] Justice Black warned that sweeping national security rationales could "wipe out the First Amendment" by placing it on the slippery slope of censorship:

> "The word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic. The Framers of the First Amendment, fully aware of both the need to defend a new nation and the abuses of the English and Colonial

---

45 4 William Blackstone, COMMENTARIES ON THE LAWS OF ENGLAND 151-52 (William Draper Lewis, 2007) (1765-69) ("The liberty of the press is indeed essential to the nature of a free state; but this consists in laying no previous restraints upon publications, and not in freedom from censure for criminal matter when published.").

46 James Madison, *Report on the Resolutions* (Feb. 7, 1799), *in* 6 THE WRITINGS OF JAMES MADISON 341, 386 (Gaillard Hunt ed., 1906).

47 *Id*. at 386

48 376 U.S. 254 (1964).

49 Jonathan Turley, *Harm and Hegemony: The Decline of Free Speech in the United States*, 45 Harvard Journal of Law and Public Policy (forthcoming 2021)

50 403 U.S. 713 (1971) (per curiam).

51 *Id*. at 728 (Stewart, J., concurring).

52 *Id*. at 724.

> governments, sought to give this new society strength and security by providing that freedom of speech, press, religion, and assembly should not be abridged."

Even with his strong view of the necessity of secrecy, Stewart noted that sacrificing the protections of the press was too costly for our constitutional system:

> "In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry—in an informed and critical public opinion which alone can here protect the values of democratic government. For this reason, it is perhaps here that a press that is alert, aware, and free most vitally serves the basic purpose of the First Amendment. For without an informed and free press there cannot be an enlightened people."[53]

The allegations contained in the New York Times report are precisely the type of information that is meant to be protected under these cases. Yet, it was also based on the disclosure of classified information. Historically, as shown in the Pentagon Papers case, some of the most important disclosures of the press have involved classified information. Indeed, the government has often classified information that is embarrassing or incriminating as it did in the Area 51 litigation.

There are a wide variety of laws that can be used for such searches. The removal or disclosure of such information is clearly a crime by those who are the sources of these articles. As a result, the mere publication of the information is confirmation of a criminal act and thus a basis for warrants and subpoenas. The 1917 Espionage Act, 18 U.S.C. §793(g), criminalizes the receipt of classified information. There are also provisions criminalizing "aiding and abetting" such disclosures. Section 798 of Title 18 also makes it a crime for anyone who "knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information [concerning communications intelligence or devices or processes]."[54] There are comparably fewer protections for the press. For example, the Privacy Protection Act of 1980[55] protects reporters from some searches and seizure of work product and materials. However, there is an exception for involvement in the alleged underlying criminal conduct.

Politicians, particularly presidents, have long professed fealty to the free press. However, attacks on the media have increased in the last twenty years. The Obama Administration prosecuted more "leakers" under the Espionage Act than any prior administration and targeted journalists and their family like James Rosen.[56] Even after the past scandals like the Rosen investigation, the current controversy may reveal the same lack of care and consultation. Despite opposing federal

---

53 *Id*. at 728.

54 18 U.S.C. 798.

55 42 U.S.C. § 2000aa, et seq.,

56 Ann E. Marimow, *Justice Department's Scrutiny of Fox News Reporter James Rosen in Leak Case Draws Fire*, Wash. Post, May 20, 2013, *available at* https://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html?utm_term=.6539d44c6ca6.

shield laws in past years, the Justice Department continues to menace the media in these cases through searches that seem little more than fishing expeditions. The media has few protections due to the curtailment of journalistic or reporter's privilege in the courts.

While closely divided, the decision in *Branzburg v. Hayes* devastated efforts to establish a robust privilege as a defense in such cases. It held that reporter Paul Branzburg could be forced to testify before state grand juries about his confidential sources.[57] While the defendant argued for a qualified, not absolute, privilege, the Court was strikingly cavalier about the need for a constitutionally grounded privilege. Justice White declared that the First Amendment "does not invalidate every incidental burdening of the press."[58] He added that "we cannot accept the argument that the public interest in possible future news about crime from undisclosed, unverified sources must take precedence over the public interest in pursuing and prosecuting those crimes reported to the press by informants and in thus deterring the commission of such crimes in the future."[59] Notably, the majority recognized that some states had already passed shield laws but cited the failure of Congress to pass such protections as an indication of a lack of need for such protections[60] – a facially absurd rationale given the fact that members of Congress are more often the subjects not the supporters of investigative journalists.

In his dissent, Justice Stewart (joined by Justices Brennan and Marshall) rebutted the dismissive treatment of the majority and warned that the lack of a journalistic privilege would "impair performance of the press' constitutionally protected functions."[61] The costs of such denial of evidence, he argued, paled in comparison to the loss of "full and fair flow of information to the public."[62] While Stewart argued for a qualified privilege, Justice Douglas argued for an "absolute and unqualified" privilege.[63] Douglas feared that a qualified privilege would be "twisted and relaxed so as to provide virtually no protection at all."[64] Under Stewart's approach, the burden would be on the government to show (1) "that there is probable cause to believe that the newsman has information that is clearly relevant to a specific probable violation of law;" (2) "that the information sought cannot be obtained by alternative means less destructive of First Amendment rights;" and (3) that there is a "compelling and overriding interest in the information."

This left the concurrence by Justice Powell, who stated that courts could balance any claim of privilege against "the obligation of all citizens to give relevant testimony with respect to criminal conduct."[65] Under Powell's test, the burden would effectively rest with the media, which would be effectively left without any reliable evidentiary privilege to protect their sources. That is why many states created such protections statutorily through shield laws. It is also why circuits have struggled to carve out a qualified privilege in the wake of *Branzburg*.[66] It is also why the Congress should, belatedly, do the same.

---

57 408 U.S. 665 (1972).
58 *Id.* at 682.
59 *Id.* at 695.
60 *Id.* at 691 n.28.
61 *Id.* at 725 (Stewart, J., dissenting).
62 *Id.*
63 *See id.* at 712 (Douglas, J., dissenting).
64 *Id.* at 720.
65 *Id.* at 710 (Powell, J., concurring).
66 *See generally The New York Times Co. v. Gonzales*, 459 F.3d 160 (2d Cir. 2006)

III. THE NEED FOR A FEDERAL SHIELD LAW

The state legislatures have shown greater concern for press freedom than Congress. Sixteen states and the District of Columbia adopted the type of absolute privilege advocated by Justice Douglas. Another twenty-four states have adopted qualified privileges along the lines of Justice Stewart. Other states recognize privilege as a matter of common and state constitutional law. There is considerable variety in these laws with exceptions and qualifications, but forty states afford express protections for reporters in resisting demands for evidence.[67] This includes such distinctions as protected confidential sources as opposed to nonconfidential material.[68] Even with these laws, the media is reporting a sharp increase in subpoena demands in civil and criminal cases.[69]

The Free Flow of Information Act of 2017 (H.R. 4382) adopts the qualified immunity approach. The legislation is clearly a major enhancement for press rights, though it could be strengthened further in my view. There could be language creating a greater presumption against compelled disclosures. It also leaves unclear the relative weight that national security claims should have in these balancing determinations. The bill simply states that "[f]or purposes of making a determination under subsection (a)(4), a court may consider the extent of any harm to national security." That offers little guidance for a court and does not address the specific issues that arise in these cases, including the ability of counsel to see evidence in classified cases or the involvement of the Foreign Intelligence Surveillance Act courts.

My primary concern is with the definition of a journalist. The legislation defines a covered person as including:

> "a person who regularly gathers, prepares, collects, photographs, records, writes, edits, reports, or publishes news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public for a substantial portion of the person's livelihood or for substantial financial gain and includes a supervisor, employer, parent, subsidiary, or affiliate of such covered person."

The definition tracks some laws but it would exclude a rising number of citizen journalists, bloggers, and others. To be honest, this is no easy task but this definition would leave most writers unprotected. Media is changing around the world. There is a shift from the classic hardnosed reporter sent on a story by a veteran editor. Most people today receive their news in substantial part from non-traditional media sources, particularly Internet sites and bloggers. These "Net-Newsers" are mixing Internet and traditional new sources.[70] For their part, traditional

---

[67] *See Number of States with shield law climbs to 40*, Reporters Comm. For Freedom of the Press, available at: https://www.rcfp.org/journals/number-states-shield-law-climbs/.

[68] See generally Jonathan Peters, *Shield Laws and Journalist's Privilege: The Basics Every Reporter Should Know*, COLUM. JOURNALISM REV. (Aug. 22, 2016), https://www.cjr.org/united_states_project/journalists_privilege_shield_law_primer.php.

[69] Sarah Matthews, Reporters Comm. For Freedom Of The Press, *Press Freedoms In The United 2019*, at 1-5 (2020), https://www.rcfp.org/wp-content/uploads/2020/03/2020-Press-Freedom-Tracker-Report.pdf.

[70] *Key News Audiences Now Blend Online and Traditional Sources*, Pew Research Center, August 17, 2008, available at https://www.pewresearch.org/politics/2008/08/17/key-news-audiences-now-blend-online-and-traditional-sources/.

reporters have become more like bloggers with social media and Internet postings. Today more people get their news for social media than newspapers.[71] The bill's definition of a covered person remains frozen in the journalistic amber of prior years. Similarly, states like California define covered persons as "[a] publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service, or any person who has been so connected or employed."[72] The federal bill is less rigid but still wedded to a narrow and frankly dated view of journalism. As previously noted, journalistic privilege has been defended by Supreme Court justices as protecting the "full and fair flow of information to the public."[73] The full array of information now flows through many sites that would not be covered by this law.

It is also unclear what a "substantial portion of the person's livelihood" means beyond eliminating those journalists who take little compensation for their work. For example, you may have someone who volunteers as a journalist without taking a salary to assist sites struggling to survive. Likewise, if Ted Koppel were to continue to write for a blog after retiring from any network, would he no longer be a journalist because he was not making money from his work? It would seem like a better definition would focus on the character and function of the work as opposed to the financial gain derived from it.

Moreover, it is not clear why it is important for protecting journalism that a protected person have "a supervisor, employer, parent, subsidiary, or affiliate of such covered person." A figure may be forced out of a news organization or simply choose to operate alone. New technology has allowed far greater freedom for journalists in reaching a global audience without the affiliation or costs of a traditional news organization. That person can still continue to write in that capacity as an independent writer and researcher. Under the common definition, a person literally becomes a non-journalist when they leave a newsroom to continue to write the same type of columns on a blog.[74]

The definition in H.R. 4382 tracks some state laws. Even states like New York which used more verbose treatments are still tied to traditional publications and a showing of working for "gain or livelihood" rather than information dissemination:

> "one who, for gain or livelihood, is engaged in gathering, preparing, collecting, writing, editing, filming, taping or photographing of news intended for a newspaper, magazine, news agency, press association or wire service or other professional medium or agency which has as one of its regular functions the processing and researching of news intended for dissemination to the public; such person shall be someone performing said function

---

[71] Social Media Outpaces Print Newspapers in the U.S. as News Source, Pew Research, Dec. 10, 2018, available at https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

[72] Cal. Evid. Code § 1070 (West 2018).

[73] *Branzburg*, 408 U.S. at 725 (Stewart, J., dissenting).

[74] Many blogs have a readership that far exceeds newspapers. For example, I would likely meet the definition due to my position as a legal analyst with a network. However, my blog (Res Ipsa) has a modest circulation but still reaches millions of readers each year and can top roughly a quarter of a million in a single day. However, a writer for a small-town newspaper reaching a couple thousand readers would still be viewed as a journalist under this definition but most bloggers (including writers for even larger blogs) would not since many of us do not accept advertising on our blogs.

> either as a regular employee or as one otherwise professionally affiliated for gain or livelihood with such medium of communication."[75]

One aspect of the New York law that is notable (and in my view worth considering) is a differentiation between "confidential news" (which receives the protections of an absolute privilege) and "nonconfidential news" (which receives the protection of a qualified privilege).

Some states have broader definitions like Montana. In *Tracy v. City of Missoula*, a court considered a motion to quash a subpoena by a student journalist who filmed a meeting of the Hell's Angels Motorcycle Club for a documentary film.[76] The film captured a scene of a confrontation with police. Montana is one of the states with an absolute protection for "any person connected with or employed by" any agency responsible for "disseminating news."[77] The student journalist prevailed in the challenge. Nebraska also covers any person "engaged in procuring, gathering, writing, editing, or disseminating news or other information to the public."[78] Likewise, the model language put forward by media groups encompasses "any person in journalism or an affiliate or assistant thereof, as well as any person for whom protection would be 'in the interest of justice' or would facilitate legitimate newsgathering."[79]

I would strongly recommend a broadening of the definition of a covered person in the federal law. Specifically, Congress should allow a court to extend any privilege to non-traditional journalists by focusing on the work itself rather than the compensation received for that work. In the end, any federal shield law would likely be a great improvement but Congress should consider whether it is basing the law on an outdated and artificially narrow concept of journalism.

IV. CONCLUSION

Fifteen years ago, I warned that, without the protections of a federal shield law, we would undermine not only the free press but also its critical function in our constitutional system. Congress has thus far failed to act to protect journalists at the time that we need them the most. Indeed, recent years have only reaffirmed, if not magnified, the importance of the media in our constitutional scheme. We cannot afford to allow our press to be targeted without additional statutory protections. Without congressional action, reporters will face an increasingly difficult environment in which to report on alleged abuses and crimes by the government. With the loss or harassment of the press reporting on these controversies, the public will be left increasingly in the dark at a time when we must be most vigilant in the protections of our rights. It will indeed be, as Madison warned, "a Prologue to a Farce or a Tragedy; or perhaps both."

---

[75] CIV. RIGHTS § 79-h(a)(6).

[76] Tracy v. City of Missoula, 2001 MT 1171, 2001 Mont. Dist. LEXIS 3168, at *21, *23, *36-40 (Dist. Ct. Missoula Cty. Mar. 9, 2001).

[77] MONT. CODE ANN. §§ 26-1-901 to -903 (West 2019).

[78] NEB. REV. STAT. ANN. § 20-146 (West 2020).

[79] MODEL QUALIFIED SHIELD LAW § 7 (MEDIA L. RES. CTR. 2014), http://medialaw.org/images/stories/Article__Reports/Committee_Reports/2014/Model_Shield_Law/modelshield2014.pdf

Thank you for the opportunity to speak with you today and I would be happy to answer any questions that you might have at this time.

Jonathan Turley
Shapiro Professor of Public Interest Law
George Washington University Law School
Washington, D.C. 20052
(202) 994-7001

Chair NADLER. Thank you for your testimony.
Ms. Oberlander, you may begin.

TESTIMONY OF LYNN OBERLANDER

Ms. OBERLANDER. Chair Nadler, Ranking Member Jordan, and Members of the Committee, thank you inviting me to testify today.

We have learned in the last few weeks that the Justice Department has secretly sought the email and telephone records of eight journalists who work for three media companies in what appears to be a purposeful attempt to evade the protections of the law and of the Department's own guidelines.

As a longtime media lawyer who has worked in many newsrooms and with hundreds of journalists, I can report that these actions have had and will continue to have a profound and disruptive effect on the ability of journalists to practice their craft and to report stories of vital public importance to our democracy.

By sending secret subpoenas to the service providers for *The New York Times*, *The Washington Post*, and CNN and then by gagging the recipients, the Department of Justice performed an end run around the protections for the news media provided in both the Privacy Protection Act of 1980 and the Attorney General's own news media guidelines.

Had the subpoenas come directly to the media organizations or if they had been notified at the time of their issuance, the media organizations would have been able to challenge them in court. Instead—and even though the prosecutors were seeking three-year-old records for an already-public leak investigation—the Department of Justice was able to convince a magistrate judge in at least one of the cases that informing the journalists of the request would, quote, "seriously jeopardize the ongoing investigation by giving targets the opportunity to destroy or tamper with evidence."

Congress should now act to more fully protect the rights of journalists to bring crucial information to the public. The honorable Members of the Judiciary Committee should consider several legislative enhancements.

The strongest and simplest way to protect the rights of journalists to report on the actions of government and the rights of the public to receive such reporting would be to pass legislation banning governmental inquiries into journalist sources, as Attorney General Garland has now said that he would strive to do. This would be the simplest response and would demonstrate the importance of the free flow of information to the public.

Even in the absence of such a ban, there are other ways to improve protections for journalistic process. Independent judicial review of any prosecutorial attempt to access journalist materials is crucial. Ensuring that it's a stringent review that appropriately weighs the public's interest in news gathering with the government's interest in uncovering a source is central to protecting the important First Amendment interests that are at stake here.

While the current Attorney General guidelines are not perfect and, crucially, are not enforceable by journalists, they provide an excellent starting point in looking to strengthen the legislative protections. The guidelines recognize that, quote, "freedom of the press can be no broader than the freedom of members of the news media

to investigate and report the news," and note that subpoenas and search warrants are "extraordinary measures, not standard investigatory practices." To this end, all such process may be issued only with the approval of the Attorney General or another senior official and only when the information sought is essential to a successful investigation, after all reasonable attempts have been made to obtain the information from alternative sources, and after negotiation and notice with the affected members of the news media. These protections should now be statutorily enacted.

The government must provide notice to the news media whenever information is sought, whether it's directly sought from the media itself or from their service providers. It is an accident of technology that the government is able to bypass the affected journalists. If the media company maintained its own email servers, for example, it would be impossible to seek the records without notice.

Notice provides an opportunity for the affected media to seek judicial review from an Article III Judge and to challenge the government's purported rationales for seeking the information.

The Department of Justice believes that prior notice and negotiation is impossible in certain cases, particularly where it threatens grave harm to national security or the investigation's integrity. In such extremely limited cases, Congress should consider legislating a duty of candor, an affirmative obligation to notify the third-party providers that it is seeking journalist materials, and not to hide the request within a broader request, as was apparently the case with a subpoena to Apple for information about Members of Congress and their staffs.

Congress should also consider requiring a confidential advocate to represent the media's interests before the court considering the application for the subpoena, the court order, or other process. This would not be unique. The USA FREEDOM Act permits a similar type of special advocate in proceedings before the FISA court.

Finally, this moment presents an excellent opportunity to pass a strong statutory shield law that would codify protection for journalists and mandate a consistent test for when, if ever, the government or private individuals can seek journalist work product and the identity of confidential sources.

Today's patchwork of shield laws and conflicting standards of protection between the State and Federal courts leads to inconsistent results and prevents journalists from adequately informing their sources of the risks they face in coming forward with crucial information for stories of public importance.

Truly a fourth estate to our tripartite government, the press, protected by the First Amendment, stands as an essential bulwark of our constitutional arrangement. Congress can help the press serve its vital role in our democracy. I urge you to do so.

Thank you.

[The statement of Ms. Oberlander follows:]

Testimony of Lynn B. Oberlander[1]
Before the House Committee on the Judiciary

"Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power"

June 30, 2021

Mr. Chairman, and Members of the Committee. Thank you for inviting me to testify today. We have learned in the past few weeks that the Justice Department has secretly sought the email and telephone records of eight journalists, working for three media companies, in what appears to be a purposeful attempt to evade the protections of the law and of the Department's own guidelines. These actions have had – and will have if allowed to continue – a profound and disruptive effect on the ability of journalists to practice their craft, and to report stories of vital public importance to our democracy. Based on my decades of experience as a lawyer in newsrooms and counseling reporters around the country who are bringing news and information to your constituents, I am here to attest to the importance of confidential sources in bringing matters of great public interest to light, and to the detrimental impact of secret attempts to discover those sources. In this written testimony, I will also propose several ideas for legislative responses.[2]

The Current State of Affairs

When the founders drafted the First Amendment, surely far from their minds was a series of laws that permitted the government, in all its might, to secretly demand from communications companies the records of members of the press, and then in many circumstances, gag those companies from ever letting the press know. If sunshine is the best disinfectant, it is obvious that this shadowy state of affairs allows for all manner of dark things to grow. And indeed, in the last few weeks, we have seen evidence of a rash of prosecutorial overreach. But in fact it is not the

---

[1] Of counsel, Ballard Spahr LLP, https://www.ballardspahr.com/People/Attorneys/O/Oberlander-Lynn.

[2] Any opinions expressed in this testimony are my own and are not necessarily those of my law firm or its clients. The historical portions of my testimony are substantially derived from numerous "friend-of-the-court" briefs submitted by my colleagues on behalf of coalitions of media organizations to the United States Supreme Court in *Risen v. United States*, No. 13-1009, 2014 WL 1275185, and *Miller v. United States* and *Cooper v. United States*, Nos. 04-1507, 04-1508, 2005 WL 1199075; from my column, *The Law Behind The AP Phone Record Scandal*, published by The New Yorker on May 14, 2013, https://www.newyorker.com/news/news-desk/the-law-behind-the-a-p-phone-record-scandal; from prior testimony by former Ballard Spahr LLP attorney Lee J. Levine before a committee of the House considering reporter's shield legislation, *see Shielding Sources: Safeguarding the Public's Right to Know, Joint Hearing Before Subcomm. of the H. Comm. on Oversight & Gov't Reform*, 115th Cong. 10-28 (July 24, 2018) (Statement of Lee Levine), https://docs.house.gov/meetings/GO/GO27/20180724/108595/HHRG-115-GO27-Wstate-LevineL-20180724.pdf; and relevant chapters from the Fifth Edition of a treatise co-authored by my Ballard Spahr colleagues entitled *Newsgathering and the Law*. I want to thank my Ballard Spahr colleague Mara Gassmann for assisting me in the preparation of this testimony.

first time that the Department of Justice has secretly sought journalists' records. Nor, if Congress declines to act, will it be the last. In 2013, I wrote a column for The New Yorker, of which I was then General Counsel, about the secret Justice Department subpoena for several months of Associated Press phone records, for more than 20 office and home telephone lines of reporters.[3] The Department did this without AP's knowledge. This was an egregious case, and likely a violation of the Department of Justice's own guidelines, but not an isolated one. Around the same time, it was revealed that the Department, in the course of an investigation of alleged leaks related to North Korea, secured a search warrant for the emails of James Rosen, a Fox News correspondent, without his knowledge.[4] The application for the warrant asserted that Rosen was an "aider, abettor and/or co-conspirator" in the potential violation of the Espionage Act, specifically to get around the broad prohibition on search warrants for newsrooms and journalists found in the Privacy Protection Act of 1980.[5] The public outcry that resulted from the AP subpoenas and the Rosen search warrant[6] prompted the Department to revise its internal guidelines governing the use of compulsory process to secure such records from a journalist's or news organization's service providers, known as its Policy regarding obtaining information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media, 28 CFR § 50.10 (the "News Media Guidelines" or "Guidelines").[7]

---

[3] Lynn Oberlander, *The Law Behind The AP Phone Record Scandal*, NewYorker.com (May 14, 2013), https://www.newyorker.com/news/news-desk/the-law-behind-the-a-p-phone-record-scandal; *see also* Charlie Savage, *Phone Records of Journalists Seized by U.S.*, N.Y. Times (May 13, 2013), https://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html.

[4] Application for Search Warrant dated May 28, 2010 & Aff. of Reginald Reyes in Support, *USA v. Email Account Redacted@Gmail.com*, No. 1:10-mj-00291 (D.C. Cir., unsealed Nov. 7, 2011) (Dkt. Nos. 20 & 20-1); *see also* Jonathan Capehart, *Regrets, Eric Holder has a few*, Wash. Post (Oct. 31, 2014), https://www.washingtonpost.com/blogs/post-partisan/wp/2014/10/31/regrets-eric-holder-has-a-few/?utm_term=.afb411750c1a.

[5] The Privacy Protection Act of 1980, 42 U.S.C. § 2000aa, *et seq.*, protects reporters and newsrooms from certain government searches. Specifically, it bars the government from compelling journalists to turn over to law enforcement work product and documentary materials, including sources, prior to publication, absent one of the statutory exceptions. One of those specified exceptions is involvement in the alleged underlying criminal conduct.

[6] *See* Editorial Board, *Another Chilling Leak Investigation*, N.Y. Times (May 21, 2013), https://www.nytimes.com/2013/05/22/opinion/another-chilling-leak-investigation.html?_r=0.

[7] *See* Lynn Oberlander, *Holder's New Rules for Pursuing Reporters*, NewYorker.com (July 13, 2013), https://www.newyorker.com/news/news-desk/holders-new-rules-for-pursuing-reporters; *Justice Dep't tightens guidelines on reporter data*, Associated Press (July 12, 2013), https://www.ap.org/ap-in-the-news/2013/justice-dept-tightens-guidelines-on-reporter-data. *See also DOJ Report on Review of News Media Policies* (July 12, 2013), https://www.justice.gov/sites/default/files/ag/legacy/2013/07/15/news-media.pdf. The Guidelines were revised in February 2014 and again in January 2015. *See* 28 C.F.R. § 50.10; *see also* Off. of the Attorney Gen., *Updated Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media* (Jan. 14, 2015), https://www.justice.gov/file/317831/download; *DOJ Justice Manual* §

The News Media Guidelines begin with the principle that "Because freedom of the press can be no broader than the freedom of the news media to investigate and report the news, the Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering activities."[8] Calling law enforcement tools such as subpoenas, court orders issued pursuant to 18 U.S.C. § 2703(d) or 3123, and search warrants to seek information from members of the news media "extraordinary measures" and not "standard investigatory practices," the Guidelines establish that the prosecutors must get permission from the Attorney General or another senior official prior to their issuance. The Guidelines also state that the information must be "essential to a successful investigation, prosecution or litigation"; that all reasonable alternative methods of seeking the information have been pursued; and that notice and negotiation with the affected member is presumed, subject to narrow exceptions when such notice and negotiation "would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm." And where prior notice is not given, the Department must notify the affected media within 45 days of the return of process, with one additional 45-day period permitted.[9]

Despite the revisions to the Guidelines and the change in Administrations, the practice of secretly obtaining journalists' records continues.[10] In 2018, the Justice Department revealed that it had secretly procured years' worth of phone and email records of *New York Times* reporter Ali Watkins in furtherance of its investigation of a Congressional aide.[11] It remains unclear whether the Department complied with its own guidelines when it did so.[12]

9-13.400 (updated Jan. 2020), https://www.justice.gov/usam/usam-9-13000-obtaining-evidence#9-13.400.

[8] 28 CFR § 50.10(a)(1).

[9] *Id.* § 50.10(a)(3), (e)(3).

[10] Most courts that have considered the issue have held that the Guidelines are not judicially enforceable by journalists. *See, e.g.*, *In re Grand Jury Subpoena (Miller)*, 397 F.3d 964, 974-75 (D.C. Cir. 2005); *In re Special Proceedings*, 373 F.3d 37, 43-44 (1st Cir. 2004); *In re Shain*, 978 F.2d 850, 853-54 (4th Cir. 1992).

[11] *See* Adam Goldman, et al., *Ex-Senate Aide Charged in Leak Case Where Times Reporter's Records Were Seized*, N.Y. Times (June 7, 2018), https://www.nytimes.com/2018/06/07/us/politics/times-reporter-phone-records-seized.html. According to the *Times*, the records were obtained through subpoenas to telecommunications companies, including Google and Verizon, and that "[i]t appeared that the F.B.I. was investigating how Ms. Watkins learned that Russian spies in 2013 had tried to recruit Carter Page, a former Trump foreign policy adviser," a subject on which she had published reports. *Id.*

[12] Editorial Board, *The Justice Department's seizure of a reporter's records could signal a dangerous campaign*, Wash. Post (June 13, 2018), https://www.washingtonpost.com/opinions/the-justice-departments-seizure-of-a-reporters-records-could-signal-a-dangerous-campaign/2018/06/13/ba3aa04a-6d9b-11e8-afd5-778aca903bbe_story.html?utm_term=.84b56c1ad4e3 ("Under Justice guidelines, hammered out between 2013 and 2015, the government should use subpoena power, court orders or search warrants for journalists' records only as extraordinary measures, not as normal investigatory tools,

And now in the latest example, we have learned that the Trump Administration served such secret subpoenas for the records of CNN, the Washington Post, and The New York Times. And when the news organizations were finally notified of the subpoenas, which the government resisted, the in-house counsel for CNN and the Times were placed under gag orders precluding them from revealing the proceedings to their own client-colleagues. This state of affairs is untenable, as it placed the lawyers in an extremely difficult position, as surely any member of the bar can understand.

The public suffers most from these government overreaches. The public relies on a free press to inform them about a multitude of important matters, not least what their government is doing. Sources, including confidential sources, are a vital part of the information ecosystem that keep the balance of powers in check within government and ensure citizens can hold their leaders accountable.

Confidential Sources: Why They Matter

Congress' efforts to curtail secret subpoenas and enact reporter's privilege legislation could have real, tangible effects. Confidential sources are often essential to the press's ability to inform the public about matters of vital concern. The current uncertainty regarding the existence and scope of a reporter's privilege in the federal courts[13] and the latest slew of secret subpoenas threaten to jeopardize the public's ability to receive such information. As the Supreme Court has recognized, the press "serves and was designed to serve [by the Founding Fathers] as a powerful antidote to any abuses of power by governmental officials."[14] The historical record demonstrates that the press cannot effectively perform this constitutionally recognized role without some assurance that it will be able to maintain its promises to those sources who will speak about the public's business only following a promise of confidentiality.

Journalists must occasionally depend on confidential sources to report stories about the

---

and, except in unusual circumstances, the government should give reporters advance notice of a bid for records, to allow sufficient time for a protest or negotiation. . . . In light of the guidelines, was the broad sweep for Ms. Watkins's communications really necessary? Or is the Justice Department using a vacuum-cleaner approach?"). DOJ refused to provide details on its practices in response to an inquiry from Senator Ron Wyden regarding the number of times in the prior five years the Department had used "subpoenas, search warrants, national security letters, or any other form of legal process authorized by a court" to collect information about journalists in the United States or American journalists abroad. *See* Ramya Krishnan, *More questions than answers from DOJ letter about journalist surveillance*, Columbia J. Rev. (July 13, 2018), https://www.cjr.org/united_states_project/surveillance-justice-department-reporters-sessions.php; Letter from Stephen E. Boyd, Assistant Attorney Gen., U.S. Dep't of Justice, to Hon. Ron Wyden, U.S. Senate (Mar. 5, 2018), https://s3.documentcloud.org/documents/4596074/3-5-18-Boyd-Letter-to-Wyden.pdf.

[13] *See* Lee Levine et al., *Newsgathering & The Law*, Chs. 18-21 (5th ed. 2018); *Shielding Sources: Safeguarding the Public's Right to Know, Joint Hearing Before Subcomm. of the H. Comm. on Oversight & Gov't Reform*, 115th Cong. 10-28 (July 24, 2018) (Statement of Lee Levine), https://docs.house.gov/meetings/GO/GO27/20180724/108595/HHRG-115-GO27-Wstate-LevineL-20180724.pdf.

[14] *Mills v. Alabama*, 384 U.S. 214, 219 (1966).

operation of government and other matters of public concern. According to recent research by the Pew Research Center, 82% of U.S. adults responded that there are times when it is acceptable for journalists to rely on unnamed sources.[15] While there is healthy ongoing debate within the journalism profession about the appropriate uses of confidential sources, nearly all agree that they are at times essential to effective news reporting.[16] As then-Congressman Mike Pence testified before the House Judiciary Committee in 2007, "[c]ompelling reporters to testify and, in particular, compelling them to reveal the identity of their confidential sources is a detriment to the public interest. Without the promise of confidentiality, many important conduits of information about our Government will be shut down."[17]

Indeed, in proceedings in the federal courts in recent years, journalists have convincingly testified about the important role confidential sources play in enabling them to report about matters of manifest public concern.[18] Confidential sources are not only critical to investigative

---

[15] Jeffrey Gottfried & Mason Walker, *Most Americans see a place for anonymous sources in news stories, but not all the time*, Pew Research Ctr. (Oct. 9, 2020), https://www.pewresearch.org/fact-tank/2020/10/09/most-americans-see-a-place-for-anonymous-sources-in-news-stories-but-not-all-the-time/. An examination of roughly 10,000 news media reports, conducted in 2005 by the Pew Research Center, concluded that fully thirteen percent of front-page newspaper articles relied at least in part on confidential sources. *See The State of the News Media*, at 20 (2005), http://assets.pewresearch.org.s3.amazonaws.com/files/journalism/State-of-the-News-Media-Report-2005-FINAL.pdf. The following year, Pew observed that newspapers, compared to other media, tend to showcase "more and deeper sourcing on major stories" while also tending "to rely more on anonymous sourcing." *See The State of the News Media*, at 130 (2006), http://assets.pewresearch.org.s3.amazonaws.com/files/journalism/State-of-the-News-Media-Report-2006-FINAL.pdf.

[16] Much of the debate regarding confidential sources concerns whether such sources are overused or misused. At bottom, while it is undoubtedly true that "[t]he right to remain anonymous may be abused when it shields fraudulent conduct," it remains the case that, "in general, our society accords greater weight to the value of free speech than to the dangers of its misuse." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).

[17] *Free Flow of Information Act of 2007: Hearing Before the H. Comm. on the Jud.*, 110th Cong. 32-34 (June 14, 2007) (Rep. Mike Pence), https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg36019/html/CHRG-110hhrg36019.htm; *see also id.* ("As a conservative who believes in limited Government, I know that the only check on Government power in real-time is a free and independent press. The 'Free Flow of Information Act' is not about protecting reporters. It is about protecting the public's right to know.").

[18] For example, one distinguished national security reporter has testified that:

> The purpose of [confidential reporter-source] relationships is to get and verify accurate information. In order to promote a free and candid relationship with confidential sources, I have frequently found it necessary to guarantee them anonymity in regard to information provided about classified or otherwise confidential and sensitive information. Much of the verification process could not be done without the guarantee of anonymity. Over the course of three decades, such guarantees of confidentiality when used to confirm information with multiple confidential sources, have proven to my satisfaction that this process yields more candid and accurate

journalists, but are equally important to the daily reporting of more routine news stories. Reporters regularly consult background sources to confirm the accuracy of official news pronouncements and to understand their broader context and significance. Without the ability to speak off the record to sources in the government who are not officially authorized to do so, there is substantial evidence that reporters would often be relegated to repeating to the public the "official" statements of public relations officers. For this reason, among others, news reporting based on confidential source material regularly receives the nation's top journalism awards, including the Polk Awards for Excellence in Journalism[19] and the Pulitzer Prize.[20]

> information than to rely solely or predominantly on public or official comments or documentation.

Pet. for a Writ of Cert., *Risen v. United States*, No. 13-1009 (Jan. 13, 2014) at 237a-238a (Decl. of Scott Armstrong in *In re Grand Jury Subpoena to James Risen*, No. 1:08dm61 (E.D. Va. Feb. 16, 2008)).

The testimony of other luminaries in national security reporting is the same. And as a long-time Rhode Island television reporter, who had exposed government corruption in his home state, testified before being sentenced to house arrest because he refused to comply with a court order requiring him to reveal a confidential source:

> In the course of my 28-year career in journalism, I have relied on confidential sources to report more than one hundred stories, on diverse issues of public concern such as public corruption, sexual abuse by clergy, organized crime, misuse of taxpayers' money, and ethical shortcomings of a Chief Justice of the Rhode Island Supreme Court.

Testimony of James Taricani, *Appendix B to the Brief Amici Curiae of ABC, Inc, et al.*, in *Miller v. United States* and *Cooper v. United* States, Nos. 04-1507, 04-1508, *available at* 2005 WL 1199075.

[19] Numerous recipients of the Polk Award, which honors enterprise reporting across various media and disciplines, have incorporated material or information provided by confidential sources into their reporting. *See* http://liu.edu/George-Polk-Awards/Past-Winners. In 2016, for example, the International Consortium of Investigative Journalists received the Polk Award for Financial Reporting, for its series on "The Panama Papers," relying on leaked documents to uncover corruption and money laundering. *See* https://www.icij.org/blog/2017/02/panama-papers-investigation-wins-george-polk-award/. The next year, an 18-month investigation by the AP that similarly relied on confidential sources yielded numerous published reports about slave labor in the seafood industry and went on to win both a Polk Award for Foreign Reporting and the 2016 Pulitzer Prize for Public Service. *See* https://www.ap.org/explore/seafood-from-slaves/. In 2020, The New York Times was honored for its reporting on Donald Trump's income tax information. *See* https://liu.edu/polk-awards/past-winners#2020.

[20] For example, the 1996 Pulitzer Prize for National Reporting was awarded to the *Wall Street Journal* for its articles reporting on the use of ammonia to heighten the potency of nicotine in cigarettes, which was based on information revealed in confidential, internal reports prepared by a tobacco company. *See, e.g.*, Alix M. Freedman, *'Impact Booster': Tobacco Firm Shows How Ammonia Spurs Delivery of Nicotine*, Wall St. J. (Oct. 18, 1995) at A1. In 2002, the Prize was awarded to the staff of the *Washington Post* "for its comprehensive coverage of America's war on terrorism, which regularly brought forth new information together with skilled analysis of unfolding developments." *See* https://www.pulitzer.org/winners/staff-55. The *Post*'s series was based, in significant part, on

The history of the American press provides ample evidence that the information confidential sources make available to the public through the news media is often vitally important to the operation of our democracy and the oversight of our most powerful institutions, both public and private. While the *Washington Post's* "Watergate" reporting may be the most celebrated example of journalists' reliance on such confidential sources,[21] there are numerous

---

information provided by unnamed public officials, both here and abroad. *See, e.g.*, Barton Gellman, *U.S. Was Foiled Multiple Times in Efforts To Capture Bin Laden or Have Him Killed*, Wash. Post (Oct. 3, 2001), https://www.washingtonpost.com/archive/politics/2001/10/03/us-was-foiled-multiple-times-in-efforts-to-capture-bin-laden-or-have-him-killed/c29ace2b-db37-4e84-8536-dfe1c5e4aaab/. In 2016, a South Florida *Sun-Sentinel* investigation about the death toll attributable to speeding police officers, often off-duty and in their personal vehicles, which was based in part on information provided by confidential sources, received Pulitzer's highest prize, for Public Service reporting. *See* Sally Kestin et a.l, *Speeding cops get special treatment*, Sun-Sentinel (Feb. 13, 2012), http://www.sun-sentinel.com/news/speeding-cops/fl-speeding-cops-culture-20120213-story.html. In 2018, *The New York Times* and *The New Yorker* shared the Public Service award for their articles, similarly based in significant part on information provided by confidential sources, exposing allegations of sexual assaults and related abuses in the motion picture industry. *See* Ronan Farrow, *From Aggressive Overtures to Sexual Assault: Harvey Weinstein's Accusers Tell Their Stories*, The New Yorker (Oct. 2017), https://www.newyorker.com/news/news-desk/from-aggressive-overtures-to-sexual-assault-harvey-weinsteins-accusers-tell-their-stories; Jodi Kantor et al., *Harvey Weinstein Paid Off Sexual Harassment Accusers for Decades*, N.Y. Times (Oct. 5, 2017), https://www.nytimes.com/2017/10/05/us/harvey-weinstein-harassment-allegations.html. And in 2019, a team at The Seattle Times earned the National Reporting prize for groundbreaking stories that, relying in part on unnamed sources, revealed the causes of the Boeing crashes and failures in oversight. *See* https://www.pulitzer.org/winners/dominic-gates-steve-miletich-mike-baker-and-lewis-kamb-seattle-times.

[21] Several journalists, including Bob Woodward and Carl Bernstein, were subpoenaed to reveal their confidential sources in 1973 in the context of a civil action in federal court brought by the Democratic National Committee against those allegedly responsible for the burglary of the committee's offices at the Watergate building. *See Democratic Nat'l Comm. v. McCord*, 356 F. Supp. 1394, 1397 (D.D.C. 1973). One year after the Supreme Court's decision in *Branzburg*, the district court quashed the subpoenas, explaining that it "cannot blind itself to the possible 'chilling effect' the enforcement of these broad subpoenas would have on the flow of information to the press, and so to the public." *Id.* In an affidavit submitted to the Supreme Court in support of James Risen, Bernstein testified:

> I am greatly concerned about the federal government's drive in recent years to subpoena reporters to testify about their confidential sources. Not only do I believe it is an assault on the First Amendment and the press freedoms we are guaranteed, but on an individual level, compelling the disclosure of confidential information by any reporter is certain to obstruct his future newsgathering and make it nearly impossible to do his job effectively. In my experience, confidential sources will speak only to a journalist they trust and one whom they believe is sufficiently independent of government influence and authority. If an investigative reporter is compelled by the government to testify as to confidential information, his trustworthiness, integrity and independence will likely be forever tainted and any potential sources who might have previously approached him with important information may very well be deterred.

other examples of valuable journalism that would not have been possible if a reporter could not credibly have pledged confidentiality to a source, including such reporting about the Pentagon Papers,[22] Enron,[23] Abu Ghraib,[24] the dire conditions at the Walter Reed Medical Center,[25] the use of military weapons,[26] and the Harvey Weinstein reporting which launched the Me Too

---

> I also believe, based on my professional experience, that compelled disclosure of confidential information will cause irrevocable damage to the quality of information the public receives.

Pet. for a Writ of Cert., *Risen v. United States*, No. 13-1009 (Jan. 13, 2014) at 253a-257a (Decl. of Carl Bernstein in *In re Grand Jury Subpoena to James Risen*, No. 1:08dm61 (E.D. Va.)).

[22] *N.Y. Times Co. v United States*, 403 U.S. 713, 717 (1971) (Black, J., concurring) ("[i]n revealing the workings of government that led to the Vietnam war, the newspapers nobly did precisely that which the Founders had hoped and trusted they would do"). There is now a broad consensus that there was no legitimate reason to hide the Papers from the public in the first place. Solicitor General Erwin N. Griswold, who argued the government's case, wrote some twenty years later that he had "never seen any trace of a threat to the national security from the publication." Erwin N. Griswold, *Secrets Not Worth Keeping; The Courts and Classified Information*, Wash. Post (Feb. 15, 1989), https://www.washingtonpost.com/archive/opinions/1989/02/15/secrets-not-worth-keeping/a115a154-4c6f-41fd-816a-112dd9908115/.

[23] Rebecca Smith & John R. Emshwiller, *Trading Places: Fancy Finances Were Key to Enron's Success, And Now to its Distress*, Wall St. J. (Nov. 2, 2001), at A1; Rebecca Smith & John R. Emshwiller, *Enron CFO's Partnership Had Millions in Profit*, Wall St. J. (Oct. 19, 2001), at C1; John R. Emshwiller & Rebecca Smith, *Corporate Veil: Behind Enron's Fall, A Culture of Operating Outside Public's View*, Wall St. J. (Dec. 5, 2001), at A1.

[24] 60 Minutes II, Apr. 28, 2004, www.cbsnews.com/ stories/2004/04/27/60II/main614063.shtml?CMP=ILC-SearchStories; Seymour M. Hersh, *Torture at Abu Ghraib*, The New Yorker (May 10, 2004), https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib; *See, e.g.*, Todd Richissin, *Soldiers' Warnings Ignored*, Balt. Sun (May 9, 2004), https://www.baltimoresun.com/news/bal-te.guard09may09-story.html (interviewing anonymous soldiers who had witnessed abuse at Abu Ghraib); Miles Moffeit, *Brutal Interrogation in Iraq*, Denver Post (May 19, 2004), https://www.denverpost.com/2005/06/06/brutal-interrogation-in-iraq/ (relying on confidential "Pentagon documents" and interview with a "Pentagon source with knowledge of internal investigations into prisoner abuses").

[25] *See* Dana Priest & Anne Hull, *Soldiers Face Neglect, Frustration at Army's Top Medical Facility*, Wash. Post (Feb. 18, 2007), https://www.washingtonpost.com/archive/politics/2007/02/18/soldiers-face-neglect-frustration-at-armys-top-medical-facility/c0c4b3e4-fb22-4df6-9ac9-c602d41c5bda/; Steve Vogel & William Branigin, *Army Fires Commander of Walter Reed*, Wash. Post (Mar. 2, 2007) at A01.

[26] *See, e.g.*, Walter Pincus, *Carter Is Weighing Radiation Warhead*, Wash. Post (June 7, 1977), at A5; Walter Pincus, *Pentagon Wanted Secrecy On Neutron Bomb Production; Pentagon Hoped To Keep Neutron Bomb A Secret*, Wash. Post (June 25, 1977), https://www.washingtonpost.com/archive/politics/1977/06/25/pentagon-wanted-secrecy-on-neutron-bomb-production/96a418bd-6d66-45c1-9ea3-5df52ed32c9c/; *See* Don Phillips, *Neutron Bomb Reversal;*

movement. Most recently, reporting by respected news organizations on President Trump's tax returns and ProPublica's reporting on the tax returns of the nation's richest citizens – both based on confidential documents provided by unnamed sources – have spurred criminal investigations and a call for revision of the nation's federal tax policy.[27]

These are just a few of the important stories that might not have been told were it not for the bravery of individuals who shared information with reporters on a confidential basis, and for reporters who used their training and expertise to use these sources consistent with journalism ethics.[28]

Harvard Study Cites '77 Post Articles, Wash. Post (Oct. 23, 1984), https://www.washingtonpost.com/archive/politics/1984/10/23/neutron-bomb-reversal/c7e0d7d7-2439-4a4a-83ff-0b60f66cc8aa/ (quoting former Defense Secretary Harold Brown as stating that "[w]ithout the [*Post*] articles, neutron warheads would have been deployed").

[27] *See* Jonathan Weisman & Alan Rappeport, *An Exposé Has Congress Rethinking How to Tax the Superrich*, N.Y. Times (June 9, 2021), https://www.nytimes.com/2021/06/09/us/politics/propublica-taxes-jeff-bezos-elon-musk.html; Jesse Eisinger, et al., *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, ProPublica (June 8, 2021), https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax.

[28] While this testimony focuses on modern examples of confidential sources, reliance by the press on such confidential sources is not an exclusively modern phenomenon. When the First Amendment was enacted, the Founders understood their importance to maintaining an informed citizenry:

> Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.

Talley v. California, 362 U.S. 60, 64-65 (1960). Indeed, the controversy that is credited with first establishing uniquely American principles of freedom of the press – the prosecution and acquittal of New York publisher Jon Peter Zenger on charges of seditious libel – arose out of Zenger's refusal to identify the source(s) of material appearing in his newspaper harshly criticizing New York's royal government. Even after Zenger was arrested and charged with criminal responsibility as the publisher, he maintained his refusal to disclose his "sources." *McIntyre*, 514 U.S. at 361 (Thomas, J., concurring). Similarly, in 1779, Elbridge Gerry and other members of the Continental Congress sought to institute proceedings to compel a Pennsylvania newspaper publisher to identify the author of a column criticizing the Congress. Ultimately, arguments that "'[t]he liberty of the Press ought not to be restrained'" prevailed and the Congress did not take action to compel such disclosure. *Id.* at 361-62 (citation omitted). In 1784, the New Jersey Legislature embarked on another unsuccessful effort to compel a newspaper editor to identify the author of a critical article. *Id.* at 362-63. These episodes were fresh in the mind of the Framers who, as Justice Thomas chronicled in *McIntyre*, unanimously "believed that the freedom of the press included the right to publish without revealing the author's name." *Id.* at 367.

What Congress Can Do

After many years working in and advising newsrooms, I have identified some tangible changes that could be made by Congress to improve transparency and accountability in the use of subpoenas to communications companies for the media's records. The strongest and simplest way to protect the rights of journalists to report on the actions of government and of the public to receive such reporting would be to codify President Biden's and the Attorney General's recent policy announcements that the Department of Justice will not seek journalists' records to uncover their sources.[29] And it is promising that the Attorney General last week said that he would work to do so. But even in the absence of such a law there are other ways to improve protections for the journalistic process, and give some comfort to the press that their materials will not be accessed without a full and fair opportunity to challenge the orders.

(1) Require Independent Judicial Review

Independent judicial review of prosecutorial attempts to access journalist materials is crucial to protecting the news media's First Amendment rights. The process should be adversarial, with a representative for the affected media able to counter the government's arguments for necessity of the information. As Judge Sack of the Second Circuit wrote in dissent in *New York Times Co. v. Gonzales*, "For the question… is not so much whether there is protection for the identity of reporters' sources, or even what that protection is, but which branch of government decides whether, when, and how any such protection is overcome." He further added that the majority opinion also acknowledged the need for judicial review. "Judge Winter's opinion makes clear that the government's demonstration of 'necessity' and 'exhaustion' must, indeed, be made to the courts, not just the Attorney General."[30] As there is no putting the horse back in the barn once a reporter's confidential records have been seized, there also should be a right of interlocutory review. An appeal, perhaps expedited to meet the needs of the government, is a necessary protective measure against overzealous prosecutors.

(2) Enhance Legal Process

While the current News Media Guidelines are not perfect--and crucially are not enforceable by journalists--they provide an excellent starting point in looking to strengthen legislatively the protections for journalists. The Guidelines recognize that "freedom of the press can be no broader than the freedom of members of the news media to investigate and report the

---

[29] *See* John Gerstein, *Garland backs legislation to end subpoenas for reporters' records*, Politico (June 25, 2021), https://www.politico.com/news/2021/06/25/garland-reporters-records-subpoenas-496291.

[30] 459 F.3d 160, 175 (2d Cir. 2006). The case concerned an attempt to get the New York Times' phone records in a leak investigation over the disclosure of information about a federal raid on two foundations suspected of providing aid to terrorists. When the Times refused to provide the records, the prosecutor threatened to get the records from the phone companies. The Times sought a declaratory judgment that its records were protected by the reporter's privilege. The Second Circuit ruled that the phone records were subject to the same common-law privilege as any other journalist records, but that on the facts of the case, the privilege was overcome.

news."[31] They also reflect that subpoenas and search warrants are "extraordinary measures, not standard investigatory practices."[32] To this end, all such subpoenas or process may be issued only after authorization of the Attorney General or another senior official, and only when the "information sought is essential to a successful investigation"; "after all reasonable alternative attempts have been made to obtain the information from alternative sources"; and after negotiation and notice with the affected member of the news media.[33] These protections should be now statutorily enacted.

The government must provide notice to the news media whenever information is sought, whether it is directly sought from the media itself, or from their service providers. It is an accident of technology that the government is able to bypass the journalists: if the media company maintained its own email servers, for example, it would be impossible to seek the records without notice. Notice provides an opportunity for the affected media to seek judicial review from an Article III judge, and to challenge the government's purported rationales for seeking the information.

The Department of Justice believes that there are some rare cases where prior notice and negotiation is impossible – the Guidelines specifically reference substantial threats to the integrity of the investigation; grave harm to national security; and imminent risk of death or serious bodily harm. 28 CFR § 50.10(a)(3). In such limited cases, Congress should consider legislating – at the very least -- a "Duty of Candor" – an affirmative obligation to notify third party providers that it is seeking journalist material, and not hide the request within a broader request for subscriber materials, as was apparently the case with the subpoena to Apple for information about members of Congress and their staffs.[34] The service provider can then determine how best to respond to the heightened First Amendment interests in the records.

In circumstances where the affected journalist or media entity is not provided notice, Congress should consider requiring a confidential advocate to represent the media's interests before the court considering the application for a subpoena, court order, or search warrant for journalists' material. This would not be unique, as the USA Freedom Act permits a similar type

[31] 28 CFR § 50.10(a)(1).

[32] *Id.* § 50.10(a)(3).

[33] *Id.* § 50.10(a)(3), (c)(4).

[34] Jack Nicas, et. al., *In Leak Investigation, Tech Giants Are Caught Between Courts and Customers*, N.Y. Times (June 11, 2021), https://www.nytimes.com/2021/06/11/technology/apple-google-leak-investigation-data-requests.html; Jay Greene, *Tech giants have to hand over your data when federal investigators ask. Here's why*, Wash. Post (June 15, 2021), https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/ ("the subpoena 'provided no information on the nature of the investigation and it would have been virtually impossible for Apple to understand the intent of the desired information without digging through users' accounts'").

of "Special Advocate" in proceedings before the FISA court. [35]

The standard for a magistrate judge to approve a subpoena or warrant under the Stored Communication Act is also woefully inadequate to protect journalists, as it only requires that the government provide "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought, "are relevant and material to an ongoing criminal investigation."[36] The Act should be amended to require the enhanced protections of the News Media Guidelines before a warrant or subpoena to a service provider for journalist records can issue.

In addition, Congress should consider limiting the length of time that a secrecy order under the Stored Communication Act can operate. Currently, the statute permits a court to order the service provider not to inform its customer of a request for records, but does not place an outside limit on the gag order. See 18 U.S.C. § 2705(b). The Guidelines, in contrast, require notice to the news media within 45 days from the return made pursuant to the process, with an additional 45-day delay permitted for certain compelling reasons. See 28 CFR § 50.10(e)(3).

(3) **Enact A Reporter's Shield Law**

For almost three decades following the Supreme Court's decision in *Branzburg v. Hayes*, 408 U.S. 665 (1972), subpoenas issued by federal courts seeking the disclosure of journalists' confidential sources were rare. Since the turn of the century, however, that situation has changed significantly. In the last two decades, a period that spans four presidential Administrations, a substantial number of subpoenas seeking the identities of confidential sources have been issued by federal courts to a variety of media organizations, the journalists they employ, and the third parties that provide them with telephone and email services. Over the same period of time, the federal courts have increasingly found themselves in conflict over whether, and the extent to which, either the First Amendment or federal common law provides journalists with a privilege to resist such subpoenas, a conflict that the Supreme Court has repeatedly declined to resolve.[37] In many parts of the country, the level of protection afforded a journalist to protect their sources will depend entirely on which court issues the subpoena. As a result of these phenomena, at the very moment when journalists are most in need of such protection, they are justifiably uncertain whether the law will honor the commitments they have made to protect the confidentiality of their sources. Reporters simply doing their jobs have been held in contempt and jailed.[38]

---

[35] 50 U.S.C § 1803(i); *see generally* Faiza Patel & Raya Koreh, *Enhancing Civil Liberties Protections in Surveillance Law*, Brennan Center for Justice (Feb. 27, 2020), https://www.brennancenter.org/our-work/analysis-opinion/enhancing-civil-liberties-protections-surveillance-law.

[36] 18 U.S.C § 2703(d).

[37] For a detailed description of the differing standards among the federal circuits, see *Shielding Sources: Safeguarding the Public's Right to Know, Joint Hearing Before Subcomm. of the H. Comm. on Oversight & Gov't Reform*, *supra* n. 2, at 12-15.

[38] Numerous examples were detailed at length in the 2007 testimony of former Ballard Spahr attorney Lee Levine, when he testified before this Committee when the shield bill was introduced. *See*

Moreover, the threat posed by government-issued subpoenas to journalists extends beyond the Justice Department. In 2016, for example, a filmmaker was forced to initiate his own federal action after a military prosecutor sought all 25 hours of unpublished interviews he had conducted.[39]

The states have, by and large, approached this balance differently. Forty-nine states and the District of Columbia recognize some form of reporters' privilege. Of those jurisdictions, forty, in addition to the District, have enacted shield laws. Although these statutes vary in the degree of protection they provide to journalists, they "rest on the uniform determination by the States that, in most cases, compelling newsgatherers to disclose confidential information is contrary to the public interest."[40]

This moment presents an excellent opportunity to revisit – and finally to pass – a strong statutory shield law that would enshrine protections for journalists, and mandate a consistent test for when – if ever – the government or private individuals can seek journalist work product and the identity of confidential sources. Today's patchwork of shield laws and conflicting standards of protection between state and federal courts leads to inconsistent results and prevents journalists from adequately informing their sources of the risks they face in coming forward with vital information for stories of public importance.

Conclusion

There is a palpable need for congressional action to preserve the ability of the American press to engage in the kind of important, public-spirited journalism that is often possible only when reporters are not, knowingly or unknowingly, turned into an investigative tool of the very government that the First Amendment contemplates they will hold accountable.

Free Flow of Information Act of 2007: Hearing Before the H. Comm. on the Judiciary, 110th Cong. 32-34 (June 14, 2007) (Statement of Lee Levine); *see also, e.g.*, *United States v. Sterling*, 818 F. Supp. 2d 945, 947-50 (E.D. Va. 2011), *vacated in part*, 724 F.3d 482 (4th Cir. 2013) (declining to find a privilege in criminal cases involving national security).

[39] *See* Josh Gerstein, *Feds fight bid to head off 'Serial' Bergdahl subpoena*, Politico (Aug. 7, 2016), https://www.politico.com/blogs/under-the-radar/2016/08/feds-fight-bid-to-head-off-serial-bergdahl-subpoena-226772.

[40] *Brief Amici Curiae of The States of Oklahoma, et al., Miller v. United States; Cooper v. United States*, Nos. 04-1507, 04-1508, available at 2005 WL 1317523. In addition, the Attorneys' General of thirty-four states and the District of Columbia have urged the Supreme Court to recognize a federal reporters' privilege. In doing so, the Attorneys' General noted that the States "are fully aware of the need to protect the integrity of the factfinding functions of their courts," yet they have reached a nearly unanimous consensus that some degree of legal protection for journalists against compelled testimony is necessary. *See id.* (citing *Jaffee v. Redmond*, 518 U.S. 1, 13 (1996)). Significantly, the experience of the States demonstrates that shield laws have had no material impact on law enforcement or on the discovery of evidence in judicial proceedings, criminal or civil. As the Attorneys' General explained, a "federal policy that allows journalists to be imprisoned for engaging in the same conduct that these State privileges encourage and protect" serves to undermine "both the purpose of the [States'] shield laws, and the policy determinations of the State courts and legislatures that adopted them." *Id.*

Chair NADLER. Thank you.

We will now proceed under the five-minute rule with questions, and I will recognize myself for five minutes.

Before I begin my questioning, and without objection, I will place the following into the record: A letter from over 20 civil society groups calling for reform; a statement from Frederick J. Ryan, Jr., CEO, and publisher of *The Washington Post*; a statement from Karen Kaiser, Senior Vice President, General Counsel, and Corporate Secretary of the Associated Press.

Without objection.

[The information follows:]

CHAIR NADLER FOR THE RECORD

June 18, 2021

Dear Attorney General Garland, Chairman Nadler, Chairman Durbin, Ranking Member Jordan, and Ranking Member Grassley,

The undersigned civil society organizations write to condemn the Department of Justice's surveillance of Members of Congress, their staff, and their families, and urge the Congress to investigate this matter immediately as well as enact substantive reforms to prevent such abuse in the future. This conduct—as well as recent revelations regarding surveillance of journalists—represents a significant threat to democratic society.

On June 10, the *New York Times* reported that in 2017 and 2018 the Justice Department seized communications records of Representatives Adam Schiff and Eric Swalwell, congressional staff, and family members—including a child—as part of leak investigations.[1] These records were collected using a grand jury subpoena, which does not require evidence of wrongdoing, despite the fact that they would surely reveal information about members of Congress. Using broad and intrusive surveillance to collect private information about a president's political rivals could easily lead to abuse, including fishing expeditions, and undermines the separation of powers that is so vital to a functional democracy.

Also disturbing are recent revelations that the Justice Department collected private communications records from journalists at the *New York Times*, the *Washington Post*, and CNN. This similarly misuses executive power to chill and undermine an institution we depend on to hold the government accountable. And in both cases, gag orders were deployed to keep improper surveillance activities hidden.

We are pleased the Department supported an inspector general investigation into this matter. However, while such an investigation is vital, it is not sufficient to remedy this abuse. According to Representative Schiff and congressional staff, the Justice Department has not been sufficiently forthcoming or provided important details about this matter.[2] This lack of transparency undermines public accountability. We call on the Justice Department to immediately release all relevant court filings, requests, and other records regarding surveillance that targeted members of Congress, their staff, and the media.

Congressional inquiry is also required. We commend the House Judiciary Committee for announcing that it will investigate the subpoenas. We call on both the House and Senate Judiciary Committees to hold public hearings to investigate the matter, including testimony from former Attorneys General Jeff Sessions and Bill Barr, and former Deputy Attorney General Rod Rosenstein. We call on the Justice Department to fully cooperate with any congressional subpoenas for documents and testimony.

Internal reforms and changes to Justice Department policy are insufficient to address this misconduct. Congress must also enact strong safeguards to restrict collection of private records containing sensitive information—such as communications records—as well as reform the overly permissive laws regarding gag orders, which serve to shield improper surveillance and hinder accountability.

While surveillance targeting political rivals and the press is shocking, it is sadly far from unprecedented. It is far past time to prohibit this type of unfettered surveillance that has repeatedly been abused. We hope the Justice Department will show a genuine commitment to preventing future misconduct by working

---

[1] Katie Benner, Nicholas Fandos, Michael S. Schmidt, and Adam Goldman, "Hunting Leaks, Trump Officials Focused on Democrats in Congress," *New York Times*, June 10, 2021. https://www.nytimes.com/2021/06/10/us/politics/justice-department-leaks-trump-administration.html

[2] Manu Raju, Evan Perez, Katie Bo Williams, and Paul LeBlanc, "Trump Justice Department subpoenaed Apple for data from House Intelligence Committee Democrats, sources say," CNN, June 10, 2021. https://www.cnn.com/2021/06/10/politics/house-intelligence-committee-apple-data-trump-justice-department-doj/index.html

with Congress, as well as civil rights and civil liberties advocates, in support of new statutory reforms to surveillance and gag orders.

We look forward to working with you on these important issues. If you have any questions please contact Jake Laperruque, senior counsel at the Project On Government Oversight's Constitution Project, at jlaperruque@pogo.org.

Sincerely,

Advocacy for Principled Action in Government
American Civil Liberties Union
Brennan Center for Justice at NYU School of Law
Center for Constitutional Rights
Citizens for Responsibility and Ethics in Washington (CREW)
Defending Rights & Dissent
Demand Progress
The Digital Democracy Project
Due Process Institute
Electronic Privacy Information Center
Government Accountability Project
Government Information Watch
Fight for the Future
National Coalition Against Censorship
Open Technology Institute
Open The Government
PEN America
Project for Privacy and Surveillance Accountability
Project On Government Oversight
Protect The 1st
Restore The Fourth
The Surveillance Technology Oversight Project
X-Lab

Statement from Frederick J. Ryan, Jr.
CEO & Publisher of The Washington Post
for the
June 30, 2021 House Judiciary Committee Hearing
"Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses
to Deter Prosecutorial Abuse of Power."

On May 6, 2021, The Washington Post learned that three of its reporters (two current and one former) had received terse, identically worded notices from the Department of Justice ("Department"), advising them that the Department had obtained toll records on their work, cell, and home phones covering a three-month period in 2017, as well as a Court order authorizing the Department to obtain "non-content communication records" for their Post email accounts, though no such email records were obtained. The Department subsequently disclosed that it had sought similar records from reporters at CNN and the New York Times and obtained gag orders against in-house lawyers at those media companies in connection with its efforts to obtain their email records. This series of media record seizures constitutes a significant intrusion on the First Amendment and justifies legislative action to provide enduring protections for the freedom of the press.

In the absence of a federal shield law, the sole bulwark against the misuse of governmental subpoenas to settle political scores, root out reporters' sources, or punish critical news coverage is found in the Department's longstanding policy on obtaining records of members of the news media. See 28 CFR § 50.10 (the "Guidelines"). The Guidelines, which have been in effect since the 1970s, expressly recognize that "freedom of the press can be no broader than the freedom of members of the news media to investigate and report the news," and therefore impose a variety of substantive and procedural checks – such as a legitimate nexus to the merits of a case, the unavailability of the information from other means, and personal Attorney General approval – before a media subpoena is issued. Id. at § 50.10(a)(1)-(a)(3).

One of the most critical of these protections is notice to the affected news organization, which is required in all but the most exceptional circumstances. The Guidelines recognize that media subpoenas to "non-consenting members of the news media" are "extraordinary measures" that should be available only "after negotiations with the affected member of the news media have been pursued and appropriate notice to the affected member of the news media has been provided, unless the Attorney General determines that, for compelling reasons, such negotiations or notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm." Id. at § 50.10(a)(3).

The Post and its reporters did not receive any notice whatsoever of the subpoenas for our records, making the question of "negotiations" moot – and depriving the Post of any opportunity to challenge the subpoenas or their scope in Court. It also remains unclear how the Department could have satisfied its burden to exercise these "extraordinary measures." The toll records obtained in this case were more than three years old, making it difficult to understand the

Department's basis for concluding that prior notice to the Post would have "pose[d] a clear and substantial threat to the integrity of the investigation, risk[ed] grave harm to national security, or present[ed] an imminent risk of death or serious bodily harm." So far, the Department has not provided any specifics about which of these exceptions allegedly applied, or why.

Given these facts, if the Guidelines were nonetheless complied with, it suggests that they provide inadequate protection for critical First Amendment interests. In addition to being outside the enforceability of a court, they suffer from structural infirmities such as the inherently vague "integrity of the investigation" standard, which seems self-evidently prone to prosecutorial abuse. In these cases, the Guidelines failed to protect the important underlying First Amendment interests, and instead had an unwarranted and harmful impact on the work of the Post and our journalists. Protection of our sources is critical to the Post and essential to informing the public, and subpoenas of this kind have a devastating chilling effect – particularly when conducted in secret, without the checks of an adversarial process in which the news organization can challenge their scope. Government sources who have historically come forward, at great personal risk, to protect the public and the nation by disclosing government abuses and wrongdoing are far less likely to do so when they believe that media communications are being swept up in a government dragnet.

We appreciate the steps the Biden Administration has already taken to quell some of these concerns. On June 5, 2021, the Department announced that it would no longer "seek compulsory legal process in leak investigations to obtain source information from the media doing their jobs." Then, following a June 14, 2021 meeting with the Attorney General and representatives of The Washington Post, the New York Times and CNN, the Department announced that the Attorney General would "develop and distribute to the field a memo detailing the current policy," and that "The Attorney General committed to working with members of the news media to codify the memo setting out these new rules into regulation."

We welcome the Attorney General's commitment to making changes to the Guidelines designed to further protect these First Amendment principles, but we believe more enduring protections are required. The Guidelines, even with meaningful and material changes, remain an imperfect tool to guarantee our nation's constitutional commitment to a free press – unenforceable in court, subject to unilateral revision by future administrations, and dependent entirely on the good will of the Department for implementation.

For these reasons, The Post supports durable and lasting legislative protections that help media companies serve the public by protecting the identity of their sources. This includes both statutory limitations on compulsory legal processes to obtain source information, and a federal shield law such as the Free Flow of Information Act that was considered by Congress in 2007 and 2013. We note that 40 states, plus the District of Columbia, already have statutory shield laws affording at least qualified protection for journalists' sources, and the administration of justice has not been unduly hampered in those jurisdictions. We urge Congress to take similar action and would be pleased to work with this Committee to help make it happen.

Karen Kaiser Testimony, June 2021

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY, U.S. HOUSE OF REPRESENTATIVES

Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power

June 30, 2021

STATEMENT BY KAREN KAISER,
Senior Vice President, General Counsel and Corporate Secretary for The Associated Press

Mr. Chairman and Members of the Committee on the Judiciary. Thank you for the opportunity to submit this testimony on a topic of great importance to the dedicated journalists of The Associated Press. Every day in this city, across the nation and around the world, reporters gather information of enormous importance from sources who only agree to disclose it on the condition that their identity will not be disclosed. Sources need this protection out of fear that disclosing their identity would risk their jobs, their livelihoods and in some instances, their lives, all for revealing critical information that the public deserves to know. Reporters passionately protect their confidential sources because, if they do not, their sources will stop talking, and the world will be deprived of this information. From the pre-revolutionary days when John Peter Zenger was jailed for refusing to reveal his anonymous sources who had criticized the British governor of New York, journalists have vigorously protected the confidentiality of their sources.[1]

A great deal of important reporting would never have reached the public but for information and leads provided by sources who insisted upon confidentiality—from such historically significant stories as those revealing government missteps that led to the Vietnam War,[2] illegal accounting practices that led to the downfall of Enron,[3] or abuse of detainees at Abu

[1] *See The Case of John Peter Zenger (1735)*, in *The Press on Trial: Crimes and Trials as Media Events* (Lloyd Chiasson, Jr. ed. 1997) at 8.

[2] *See N.Y. York Times Co. v. United States*, 403 U.S. 713 (1971). Solicitor General Erwin N. Griswold, who argued the government's case, wrote twenty years later that he had "never seen any trace of a threat to the national security from the publication." Erwin N. Griswold, *Secrets Not Worth Keeping; The Courts and Classified Information,* Wash. Post (Feb. 15, 1989), https://www.washingtonpost.com/archive/opinions/1989/02/15/secrets-not-worth-keeping/a115a154-4c6f-41fd-816a-112dd9908115/.

[3] Rebecca Smith & John R. Emshwiller, *Trading Places: Fancy Finances Were Key to Enron's Success, And Now to its Distress*, Wall St. J. (Nov. 2, 2001) at A1 (relying on confidential sources and leaked documents to reveal the illegal accounting practices of a company that had "routinely made published lists of the most-admired and innovative companies in America"); *see also* Rebecca Smith & John R. Emshwiller, *Enron CFO's Partnership Had Millions in Profit*, Wall St. J. (Oct. 19, 2001) at C1; John R.

Ghraib prison in Iraq,[4] to such more recent reporting of national significance as disclosures concerning police surveillance of minority populations,[5] and conditions of confinement at the border.[6] But by far the greater use of such information is reflected in day-to-day reporting on the widest range of topics. A study of roughly 10,000 news media reports several years ago concluded that fully thirteen percent of front-page newspaper articles relied at least in part on anonymous sources.[7]

These hearings are a timely response to the recent revelations that the Department of Justice had secretly sought to seize phone records and email information from reporters, members of Congress and congressional staffers in an effort to identify the sources of unwelcome leaks, even gagging the lawyers of news organizations and others along the way. Such subpoenas seeking to compel disclosure of records revealing with whom and when a communication occurred thwart the ability of journalists to credibly promise confidentiality and intimidate sources into silence. The result is loss of information to the public, and lack of ability to hold our leaders to account.

Although President Biden has now promised that such subpoenas will not be issued by his Justice Department, Congress needs to act to ensure an enduring solution to this serious threat to a free press and to the separation of powers. It is essential that reporters be able to credibly promise confidentially to ensure the public has the information needed to hold its government accountable and to help government agencies and officials function more effectively and with integrity.

Emshwiller & Rebecca Smith, *Corporate Veil: Behind Enron's Fall, A Culture of Operating Outside Public's View*, Wall St. J. (Dec. 5, 2001) at A1.

[4] *See* Seymour M. Hersh, *Torture at Abu Ghraib,* The New Yorker (May 10, 2004) (reporting on photographs graphically depicting abuse in the possession of Army officials and a classified report), https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib; Todd Richissin, *Soldiers' Warnings Ignored*, Balt. Sun (May 9, 2004), https://www.baltimoresun.com/news/bal-te.guard09may09-story.html(interviewing anonymous soldiers who had witnessed abuse at Abu Ghraib); Miles Moffeit, *Brutal Interrogation in Iraq*, Denver Post (May 19, 2004), https://www.denverpost.com/2005/06/06/brutal-interrogation-in-iraq/(relying on confidential "Pentagon documents" and interview with a "Pentagon source with knowledge of internal investigations into prisoner abuses")

[5] *See* Highlights of AP's Pulitzer Prize Winning Probe into NYPD Intelligence Operations, https://www.ap.org/about/awards-and-recognition/highlights-of-aps-pulitzer-prize-winning-probe-into-nypd-intelligence-operations

[6] *See* Nomaan Merchant, *AP exclusive leads to release of migrant kids held in US hotels for deportation*, Associated Press (July 31, 2020), https://leads.ap.org/best-of-the-week/exclusive-on-detaining-deporting-kids.

[7] *See generally State of the News Media 2005*, www.stateofthemedia.org/2005/index.asp.

The Important Interests at Stake

To shape a proper response to the current situation, it is important to be clear about what needs to be protected. It is not some abstract notion of a "free press" that needs defending, but rather the concrete ability of journalists to help us make sense of a complex world, understand the abuses of government, and make informed choices. Executive branch efforts to find leakers by seeking out the communications records of the recipients of those leaks effectively dams up historically important ways in which information reaches the public.

I can attest to that fact from AP's own experience when a leaks investigation by the Obama administration targeted its telephone records. In May 2012, AP published a story on a foiled plot by an al-Qaida affiliate in Yemen that was planning to use a bomb to destroy an airliner headed for the United States. Our story revealed that the CIA had thwarted the attack, which was intended to coincide with the anniversary of the killing of Osama bin Laden. The story was not a surprise to the U.S. government: AP had held the report for five days at government request, because the sensitive operation was still underway. Only after the administration assured us that their security concerns had been allayed did we release the story.

A year later, on May 10, 2013 the Department of Justice notified AP that it had secretly seized records for 21 AP phone lines over most of a two-month period covering the time that our story was released. This unprecedented intrusion into AP's newsgathering records by government officials was broad and overreaching. The seized records included not just the work and personal numbers of individual AP journalists, but general AP numbers in New York, Washington and Hartford, Conn., and AP's main phone number in the U.S. House of Representatives press gallery. It included incoming and outgoing calls. These were not just the phone lines of our investigative team. They were the general office numbers where as many as 100 reporters and editors worked. Thousands of phone calls were swept up. It was hardly a surgical strike on a few carefully chosen targets; it was an overbroad and sloppy fishing expedition into a wide spectrum of AP news journalists -- most of whom had little or nothing to do with the issues in question – and it revealed information that the government had no right to know about AP's operations.

The seizure of AP records had an impact beyond the specifics of the case. As AP President and CEO Gary Pruitt noted at the time, "Officials that would normally talk to us and people we talk to in the normal course of newsgathering are already saying to us that they're reluctant to talk to us… They fear that they will be monitored by the government."[8] Some longtime trusted sources

[8] Gary Pruitt, *Address to the National Press Club* (June 19, 2013), https://www.ap.org/press-releases/2013/ap-ceo-addresses-phone-records-seizure-and-safeguards.

became nervous and anxious about talking with AP reporters -- even on stories unrelated to national security. In some cases, government employees AP once checked in with regularly would no longer speak to AP reporters by phone. Others became reluctant even to meet in person. In one instance, an AP reporter could not get a law enforcement official to confirm a detail that had been reported elsewhere. The impact of the seizure on sources was swift and sure. And the chilling effect on newsgathering was not just limited to AP. Journalists from other news organizations told us that it had intimidated both official and nonofficial sources from speaking to them as well.

The impact of government monitoring of reporters' communications is not only on sources; it also has an impact on the reporters involved. For example, Eric Lichtblau shared a Pulitzer Prize with James Risen for their investigation into the NSA's illegal warrantless wiretapping program. Lichtblau has reported that once he learned "from various news sources that the FBI had been monitoring my phone and Internet communications" as part of a leak investigation arising from that story, it made it more difficult for him to do his job, worrying in dealing with confidential sources whether he might "be forced to testify before a grand jury or risk going to jail to protect a source."[9] New York Times reporter Philip Shenon, whose phone records were seized during the Bush administration recalled thinking at the time, "'My goodness, if I were one of my sources, I would never talk to me again, even about stories that really would have been a public service.'"[10]

Simply put, the "chilling effect" is real. Even the FBI understands this when the shoe is on the other foot. In 1941 Attorney General Robert Jackson declined to release investigative reports of the Federal Bureau of Investigation demanded by a congressional committee for just this reason. As he put it:

> [D]isclosure of the reports would be of serious prejudice to the future usefulness of the Federal Bureau of Investigation . . . [M]uch of this information is given in confidence and can only be obtained upon pledge not to disclose its sources. We regard the keeping of faith with confidential informants as an indispensable condition of future efficiency.[11]

Just as the FBI depends upon its ability to promise confidentiality, journalists sometimes need to promise confidentiality to report important stories about the operation of government and other matters of public concern. AP reporters sometimes even risk their lives to get the stories that

---

[9] Molly Redden, *Is the "Chilling Effect" Real*, New Republic (May 15, 2013), https://newrepublic.com/article/113219/doj-seizure-ap-records-raises-question-chilling-effect-real.

[10] *Id.*

[11] *Address by Hon. Edward H. Levi, U.S. Attorney Gen., before the Ass'n of the Bar of the City of N.Y.*, (Apr. 28, 1975), https://www.justice.gov/ola/page/file/1090496/download .

matter—particularly AP's heroic international reporters—and these journalists must promise confidentiality on occasion to get the story, and must able to uphold that promise. The following provides just a few examples of the type of ground-breaking AP stories, all of which served the public interest, that could never have seen the light of day without information provided by confidential sources:

- DEATH OF RONALD GREENE: Ronald Greene, a black man, was killed in custody by Louisiana state troopers in 2019. But the circumstances of his death remained shrouded in secrecy for two years until AP reporter Jim Mustian, relying significantly on anonymous sources, obtained bodycam video of Greene's arrest and beating, along with other details of the case, which is now the subject of a federal civil rights investigation, as well as a state investigation probing whether the state police unit involved has systematically targeted black motorists.[12]

- TIGRAY ETHNIC VIOLENCE: AP East Africa Correspondent Cara Anna and colleagues have revealed the horrifying details of an ongoing ethnic cleansing campaign in the Tigray region of Ethiopia. This reporting relied significantly on sources who asked to remain anonymous out of fear of reprisals from government and Eritrean troops carrying out the atrocities. Without their accounts, the world would know little of this distant conflict because of tight government controls on access to the region.[13]

- FAMILY SEPARATIONS AT US-MEXICO BORDER: AP reporters relied on both named and unnamed sources, as well as extensive documents and eyewitness reporting, to exclusively report details of the Trump administration's policy of separating families at the border. These included a report that administration officials were detaining children as young as 1 in hotels before deporting them; as well as an earlier accounting that showed more than 14,000 children, from infants to teens, were being detained at various facilities at that time. The latter story was a centerpiece of AP's Pulitzer finalist for national reporting in 2019.[14]

---

[12] *See* Jim Mustian, *Louisiana police unit probed over Black driver arrests*, Associated Press (June 9, 2021), https://apnews.com/article/la-state-wire-louisiana-death-of-ronald-greene-arrests-4a47c5e0ef720019d15818cf32eb2a2a; *see also* Jim Mustian, *AP Exclusive: Investigative reporter obtains bodycam video of Ronald Greene's deadly arrest*, Associated Press (May 28, 2021), https://leads.ap.org/best-of-the-week/video-of-deadly-arrest-of-black-man; Jim Mustian, AP Exclusive: Secret panel investigating Louisiana State Police unit's treatment of Black motorists, Associated Press (June 18, 2021), https://leads.ap.org/best-of-the-states/louisiana-probes-police-treatment-of-black-drivers.

[13] *See* Cara Anna, *"Leave no Tigrayan": In Ethiopia, an ethnicity is erased*, Associated Press (April 7, 2021), https://apnews.com/article/ethiopia-tigray-minority-ethnic-cleansing-sudan-world-news-842741eebf9bf0984946619c0fc15023; *see also* Cara Anna, *Determined source work exposes horrific massacre in holy city of Ethiopia's isolated Tigray region*, Associated Press (Feb. 26, 2021), https://leads.ap.org/best-of-the-week/exclusive-on-horrific-massacre-in-tigray-conflict.

[14] *See* Nomaan Merchant, *AP Exclusive: Migrant kids held in US hotels, then expelled*, Associated Press (July 22, 2020), https://apnews.com/article/weekend-reads-c9b671b206060f2e9654f0a4eaeb6388; Garance Burke & Martha Mendoza, *"A moral disaster": AP reveals scope of migrant kids program*,

- TREATMENT OF UYGHURS IN WESTERN CHINA: AP's exclusive reporting on China's treatment of its ethnic Uyghur minority relied in part on anonymous sources, who had real reason to fear for their lives for revealing that Muslim detainees in Xinjiang were subjected to forced labor in factories where they were producing sportswear and other products for US brands, and that Uyghur women were being forced by the government to undergo forced sterilization and abortions.[15]

- COVID ORIGINS: AP colleagues in China and Europe teamed up for a series of blockbuster reports last year that, with the help of confidential sources, revealed previously unreported details of China's early handing of the coronavirus pandemic that began in Wuhan. This reporting revealed the government's six-day delay in reporting the emergence of the new virus to the world, at a critical juncture where every hour counted. It also showed that China had withheld key "details from scientists at the World Health Organization who were investigating the new virus. This reporting, along with some of the Uyghur reporting noted above, was a 2021 Pulitzer finalist for investigative reporting.[16]

There can be no genuine dispute about the critical importance of a journalist's ability to promise confidentiality to informing the public about the news that matters.

Sources of the Ongoing Problem

Recent events show that the surveillance of journalists by overzealous prosecutors is an ongoing problem. It is not a partisan problem; it is not about Democratic administrations or Republican administrations. After a leak revealed that the National Security Agency had spied for years without warrants on Americans' international phone calls, the George W. Bush administration convened a grand jury and threatened to prosecute both journalists and their sources. Under the Obama administration, six government employees, and two contractors, were charged with felony criminal violations under the 1917 Espionage Act, and along the way the AP

Associated Press (December 20, 2018), https://apnews.com/article/az-state-wire-mi-state-wire-ct-state-wire-or-state-wire-wa-state-wire-a857e04de9bc4871995b65784ed7ccd8; *See also* Garance Burke et al., Two AP exclusives: China's forced labor and US detention of migrant youths, Associated Press (June 4, 2019), https://leads.ap.org/best-of-the-week/exclusives-china-forced-labor-and-us-migrant-detention.

[15] *See* Dake Kang et al., *US sportswear traced to factory in China's internment camps*, Associated Press (December 19, 2018), https://apnews.com/article/99016849cddb4b99a048b863b52c28cb; *China cuts Uighur births with IUDs, abortion, sterilization*, Associated Press (June 29, 2020), https://apnews.com/article/ap-top-news-international-news-weekend-reads-china-health-269b3de1af34e17c1941a514f78d764c.

[16] *See China didn't warn public of likely pandemic for 6 key days*, Associated Press (April 15, 2020), https://apnews.com/article/virus-outbreak-health-ap-top-news-international-news-china-clamps-down-68a9e1b91de4ffc166acd6012d82c2f9; *China delayed releasing coronavirus info, frustrating WHO*, Associated Press (June 2, 2020), https://apnews.com/article/united-nations-health-ap-top-news-virus-outbreak-public-health-3c061794970661042b18d5aeaaed9fae

phone logs were secretly seized as were the email communications of a Fox News reporter, and a New York Times reporter was ordered to testify about his source or go to jail. During President Trump's four years in office, his Justice Department filed as many indictments for leaks to the press as the Obama administration filed in eight.[17] And we now know that the Department also secretly seized records of reporters' communications and expanded its secret surveillance to the record of members of Congress, their staffs and their families.

Two factors have contributed to the pressures on even well-intentioned prosecutors to seek the communications of reporters in leak investigations: (1) a system of vast over-classification that declares criminal the disclosure of far too much information, generating far too many leak investigations, and (2) a legal system that places too much discretion in the hands of prosecutors alone, in pursuing those leak investigations. A real solution to the problem should address both.

1. Overclassification.

Information is massively over-classified in the United States, and there is longstanding, bi-partisan consensus to this effect. Every government study of the issue over the last six decades has found widespread classification of information that the government has no basis to conceal.[18] It has been estimated that as much as 50% of classified information is not properly classified.[19] The problem is not new. As former solicitor general Erwin Griswold observed long ago: "It quickly becomes apparent to any person who has considerable experience with classified material" that "the principal concern of the classifiers is not with national security, but rather with

---

[17] *See All Incidents*, U.S. Press Freedom Tracker, https://pressfreedomtracker.us/all-incidents/?categories=7 (last visited Mar. 4, 2021).

[18] *See* Def. Dep't Comm. on Classified Info., *Report to the Sec'y of Def.* 6 (1956); Comm'n on Gov't Sec., 84th Cong., *Report to the Comm'n on Gov't Sec.* 174-75 (1957); Special Subcomm. on Gov't Info., *Report of the Special Subcomm. On Gov't Info.*, H.R. Rep. No. 85-1884 (1958) at 4; Def. Sci. Bd. Task Force on Secrecy, *Report of the Def. Science Bd. Task Force on Secrecy* 2 (1970); Comm'n to Review DOD Sec. Policies & Practices, *Keeping the Nation's Secrets: A Report to the Sec'y of Def.* app. E 31 (1985); Joint Sec. Comm'n, Redefining Sec.: *A Report to the Sec'y of Def. & the Dir. Of the CIA* 6 (1994); Comm'n on Protecting & Reducing Gov't Secrecy, *S. Report of the Comm'n on Protecingt & Reducing Gov't Secrecy*, 103RD Cong., S. Doc. No. 105-2 xxi (1997); Nat'l Comm'n on Terrorist Attacks Upon the U.S., *The 9/11 Comm'n Report: Final Report of the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* 417 (2004).

[19] *See Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing*, Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, & Int'l Relations of the Comm. on Gov't Reform, 108th Cong. 263 at 82-83 (2004) (statement of J. William Leonard, Director, Information Security Oversight Office, Nat'l Archives & Records Admin.).

governmental embarrassment of one sort or another."[20] Indeed, instances of classification made in excess of authority to conceal unlawful behavior or prevent embarrassment are well-documented.[21]

The massive over classification of government information is a key component of the exponentially increasing spate of criminal leak prosecutions over the past three administrations and engenders the leak investigations in which abuses are occurring. Over classification also facilitates selective disclosures to sway public opinion. For example, The Senate Select Committee on Intelligence report on the CIA's program of enhanced interrogation detailed an "aggressive" and misleading public relations campaign fueled by choice disclosures of classified information to "make sure the impression of what we do is positive."[22] Other examples abound. The Bush administration boosted support for its plans to attack Iraq by selectively citing evidence from a classified National Intelligence Estimate (NIE) that Saddam Hussein had weapons of mass destruction and was actively pursuing a nuclear bomb.[23] During the Obama administration, debate about civil rights and liberties impacted by government surveillance, targeted killings and other issues was thwarted by the classification of information vital to those debates.[24] More recently, the CIA selectively declassified favorable documents from her time at the agency to support the nomination of Gina Haspel to be CIA Director, while damaging material about her role in the torture program remained classified and was kept from the public.[25]

---

[20] Erwin N. Griswold, Op-Ed., *Secrets Not Worth Keeping: The Courts and Classified Information*, Wash. Post (Feb. 15, 1989), https://www.washingtonpost.com/archive/opinions/1989/02/15/secrets-not-worth-keeping/a115a154-4c6f-41fd-816a-112dd9908115/.

[21] *See, e.g.*, *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 139-140 (1951) (Attorney General exceeded authority conferred by executive order; injunctive relief granted); *ACLU v. Office of Dir. Nat'l Intelligence*, 2011 WL 5563520, at *5-6, 12 (S.D.N.Y. Nov. 15, 2011) (classification to "conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment" is improper) (internal marks and citations omitted); E. Griswold, *Secrets Not Worth Keeping*, Wash. Post (Feb. 15, 1989), *supra* (the principal concern of most classifiers is "governmental embarrassment of one sort or another").

[22] S. Rept. 113-288, *Exec. Summary, S. Select Comm. on Intelligence: Comm. Study of the CIA's Detention & Interrogation Program*, 113th Cong. (Comm. Print 2014) at 403.

[23] *Key Judgments (from October 2002 NIE)*, Nat'l Intelligence Council 1 (Oct. 2002), https://fas.org/irp/cia/product/iraq-wmd.pdf [hereinafter NIE 2003 Release].

[24] *See, e.g.*, *N.Y. Times Co.*, 756 F.3d at 104-08 (surveying government efforts to shield the legal justifications relied upon in carrying out targeted killing); E. Macaskill & G. Dance, *NSA Files Decoded*, Guardian (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded (massive scale of the NSA collection of citizen's telephone and email data kept from the American public through classification).

[25] Karoun Demirjian, *CIA Declassifies Memo Clearing Haspel of Responsibility for Destroying Evidence*, Wash. Post (Apr. 20, 2018), https://www.washingtonpost.com/powerpost/cia-declassifies-memo-clearing-

I recognize that the problems of over classification are beyond the scope of this hearing, but to address fully the prosecutorial overreach in leak investigations will ultimately require meaningful reform of our system of classification as well. Congress has an important role to play in ensuring that the American people have the information they need to exercise meaningful oversight of their elected officials.

2. *Lack of judicial oversight.*

The other key structural contributor to the current problem is the largely unfettered discretion that until just recently has been afforded to the prosecutors pursuing leak investigations to decide whether to issue subpoenas that can compel phone companies and email providers to disclose records without any notice to the journalists whose records are sought and without any meaningful judicial oversight, informed by an adversarial process.

In the post-Watergate era, the Department of Justice developed regulations to guide the use of subpoenas on journalists and their work. The guidelines required federal prosecutors to (1) pursue every avenue of information available to them before issuing a subpoena to a reporter, (2) narrow any subpoena to seek only information essential to the investigation, and (3) provide advance notice to the reporter whenever possible without jeopardizing the investigation. They also required the personal approval of the attorney General for any subpoena issued to a reporter.[26]

The regulations were first proposed by Attorney General John Mitchell in 1970. They reflected a widespread recognition, in the wake of government deception during the Vietnam War, that reporters must be able to communicate in confidence with sources. Indeed, the preamble to the regulations expressly recognized "a reporter's responsibility to cover as broadly as possible controversial public issues" and the need to avoid legal process "that might impair the newsgathering function."[27] The stated goal of the regulations was "to strike the proper balance between the public's interest in the free dissemination of ideas and information and the public's interest in effective law enforcement and the fair administration of justice."[28] They had the effect

---

haspel-of-responsibility-for-destroying-evidence/2018/04/20/a79e9bfc-44de-11e8-bba2-0976a82b05a2_story.html.

[26] 28 C.F.R. § 50.10 (1999). The regulations were revised in 2014 and again in 2015 by Attorney General Eric Holder during the Obama administration to include modern forms of communication and to restrict the use of search warrants to obtain information from reporters where there is no intent to prosecute the reporter. *See Amending the Department of Justice subpoena guidelines*, Reps. Comm. for Freedom of the Press, https://www.rcfp.org/attorney-general-guidelines/.

[27] 28 C.F.R. § 50.10 (1999).

[28] *Id.*

of severely limiting the number of subpoenas issued to reporters by federal prosecutors for several decades.[29]

The problem is that the regulations as currently drafted cannot be enforced in court and the balancing can easily be tipped in favor of law enforcement. Moreover, in a leak case, where disclosure to the reporter *is* the crime, the standards in the regulation may be insufficient. In a leak case, the reporter necessarily has information essential to the investigation that is unlikely to be available anywhere else, except from the source, who is unknown. Thus, the showings required by the regulation can almost always be filled, and prosecutors may well feel that providing notice to the reporter before the subpoena is served could jeopardize the investigation. That is certainly the position the prosecutors took with AP in 2013, asserting that advance notice to AP of the seizure of its records might give the leakers time to destroy evidence, despite the fact that the underlying investigation was already well-known publicly.

In short, in a leak investigation the Justice Department regulations provide no real protection and the "balance between the public's interest in the free dissemination of ideas and information and the public's interest in effective law enforcement" is being struck by prosecutors who have a finger on one side of the balance. As District of Columbia Judge David Tatel has observed, "Because leak cases typically require the government to investigate itself, if leaks reveal mistakes that high-level officials would have preferred to keep secret, the administration may pursue the source with excessive zeal, regardless of leak information's public value."[30]

Both Judge Tatel and Second Circuit Judge Robert Sack have concluded that in the unique circumstances of a leak investigation, the balance between the public interest in prosecuting a leaker and the public's interest in preserving the flow of information enabled by confidential reporter/source relationships can only fairly be struck by an independent arbiter, which is the role of the judiciary in our system. As Judge Tatel expressed it, the "dynamics of leak inquiries afford particularly compelling reason for judicial scrutiny of prosecutorial judgments regarding a leak's harm and news value." Judge Sack has pressed the same point: "I do not think…that the executive branch of government has that sort of wholly unsupervised authority to police the limits of its own power under the[] circumstances [of a leak investigation]."

---

[29] *See Free Flow of Information Act of 2007: Hearing on H.R. 2102 Before the H. Comm. on the Judiciary*, 110th Cong. 2 (2007) (testimony of Rachel L. Brand, Assistant Att'y Gen. for the Office of Legal Policy, U.S. Department of Justice), https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg36019/html/CHRG-110hhrg36019.htm (testifying that only nineteen DOJ subpoenas to the press for confidential source information were approved between 1991 and 2007).

[30] *In re Grand Jury Subpoena, Judith Miller*, 397 F.3d 964 (D.C. Cir.) (Tatel, J., concurring), *cert. denied*, 125 S.Ct. 2977 (2005), *reissued as amended*, 438 F.3d 1141, 1176 (D.C.Cir.2006).

The Supreme Court has also embraced the concept that the judiciary should necessarily have a role in striking the proper balance between the needs of law enforcement and the needs of a free press. The Court has addressed the notion of a reporter's privilege on only one occasion, during upheavals from the Vietnam War, the Black Panther movement, and social unrest. In *Branzburg v. Hayes*[31] the Court in 1972 refused to permit reporters to assert a privilege against appearing before a criminal grand jury to testify about a confidential source.[32] But in rejecting the reporters' claim of privilege not to respond to a subpoena at all, the Court acknowledged the significant First Amendment implications presented—and five justices accepted the notion that a qualified public interest privilege should be recognized in some contexts.[33]

Justice Powell provided the crucial fifth vote and left no doubt about the important role for the courts in this situation. Powell underscored that "[t]he Court does not hold that newsmen, subpoenaed to testify before a grand jury, are without constitutional rights with respect to the gathering of news or in safeguarding their sources."[34] Although the majority rejected a blanket privilege against appearing before a grand jury, Justice Powell expressly endorsed the continuing ability of reporters to challenge specific subpoenas if they sought testimony about a confidential source "without a legitimate need of law enforcement."[35] In such cases, Justice Powell explained, a reporter could continue to assert a privilege and would have "access to the court on a motion to quash" where "[t]he asserted claim to privilege should be judged on its facts by the striking of a proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct."[36]

Simply put, the lack of guaranteed recourse to the courts can fuel prosecutorial overreach. One way to solve this is to write procedures into law that require a judge, through an adversarial process, to assess the propriety of a subpoena issued for the records of a journalist before the records are turned over.

---

[31] 408 U.S. 665 (1972).

[32] *Id.* at 706-08.

[33] *Id at* 707-08; *id.* at 709 (Powell, J., concurring) ("The Court does not hold that newsmen, subpoenaed to testify before a grand jury, are without constitutional rights with respect to the gathering of news or in safeguarding their sources."); *id.* at 712 (Douglas, J., dissenting) ("It is my view that these is no 'compelling need' that can be shown which qualifies the reporter's immunity from appearing or testifying before a grand jury, unless the reporter himself is implicated in a crime."); *id.* at 725-26 (Stewart, J., dissenting) ("The reporter's constitutional right to a confidential relationship with his source stems from the broad societal interest in a full and free flow of information to the public.").

[34] *Id.* at 709 (Powell, J., concurring).

[35] *Id.* at 709-10.

[36] *Id*. at 710.

Elements of a Better Path Forward

If reporters' phone calls become open territory for the government to monitor, then news sources will be intimidated from talking to reporters and the public will know only what the government wants it to know. This is hardly what the framers had in mind when they wrote the First Amendment. Congress should address the woefully insufficient protections in our current legal structure.

While the Biden administration has discontinued the proceedings it inherited that were seeking to obtain records of journalists, and has pledged never to seek journalist's confidential records in a leak investigation, a more certain and permanent remedy is needed. That would guarantee consistency of protections across future administrations. The following highlights for the Committee elements to consider in proposing any measure to address the current concerns.

1. ***Prohibit the use of subpoenas seeking confidential source and newsgathering information held by journalists.***

One option is to write into law the pledge of the Biden administration. Prohibit federal prosecutors from using a subpoena or any other judicial instrument to obtain information from a reporter or a reporter's telephone, internet, credit card and similar service providers that seeks to identify a confidential source or reveal information obtained in the course of professional newsgathering activity. Full stop. An exception would be in those situations where the reporter was the target of a criminal investigation for a crime other than the receipt of classified or confidential information, or for limited exigent circumstances.

2. ***At a minimum, impose procedures to ensure that such subpoenas are authorized only in the most compelling circumstances and with judicial oversight.***

The post-Watergate Justice Department regulations largely worked to protect reporters' confidential sources and newsgathering information in routine criminal cases. As New York Times reporter Adam Liptak observed in 2000, through six administrations the regulations had "remained stable and consistently enforced, even as the journalists' privilege has taken a beating in the federal courts."[37] While they are not wholly satisfactory in leaks investigations, as noted above, one element of a comprehensive set of reforms short of an outright ban of subpoenas seeking reporters information would be to enact the regulations and make them enforceable by the journalists they are intended to protect. Such an approach would mandate, among other things,

[37] Adam Liptak, *The Hidden Federal Shield Law: On the Justice Department's Regulations Governing Subpoenas to the Press*, 1999 Ann. Surv. Am. L. 227.

that the attorney general personally approve any such subpoena and that advance notice be given to the reporter *before* information is obtained, so that the reporter has an opportunity to move to quash the subpoena and an independent judge will strike the balance between the needs of law enforcement and the needs of a free press.

Notice and an opportunity to oppose is essential.

Once a reporter's records are provided to a prosecutor, the damage is done. The prosecutor can immediately identify all the reporter's confidential sources, and the subsequent return of the records cannot undo the injury. The DOJ executed its subpoena without any prior notice to AP, even though this seemed to violate the Department's rules in effect at the time because there was no apparent risk to the ongoing leak investigation by providing notice. The absence of notice, of course, meant AP could not seek judicial review of the massively overbroad subpoena before months of telephone records involving scores of AP reporters were turned over to the prosecutors.

Had the Department been required by law to provide notice, we could have helped them narrow the scope of the subpoena. If we could not agree on the proper scope, then a court would have decided which was right. Instead, under the current legal framework, the Department acts as judge, jury, and executioner -- in secret.

An impartial decisionmaker is essential.

The need for the involvement of the courts is fundamental. The courts are charged in cases involving constitutional rights, like the rights of a free press, to ensure that government action is justified in light of the constitutional interests at stake and, if justified, that it is also narrowly tailored so as not to infringe unduly on basic freedoms. There is no substantial or legitimate governmental interest in avoiding such judicial scrutiny when prosecutors seek to unmask a reporter's confidential source.

Judicial oversight is essential to ensure that proper checks and balances are maintained. In the AP phone records case, the Justice Department determined, on its own, that advance notice could be skipped, with no checks from any other branch of government. Without judicial oversight, as Judge Sack has cautioned, prosecutors "limited only by their own self-restraint" can obtain records that identify journalists' confidential sources "virtually at will."[38]

[38] *N.Y. Times v. Gonzales*, 459 F.3d 160, 175 (2d Cir. 2006).

3. Specify the heightened standard that a prosecutor must meet to obtain such a subpoena.

A federal shield law is long overdue and should be a part of effective reform to protect the flow of newsworthy information to the public. Almost every state affords such protection today. Such a law would create a statutory privilege for reporters that can only be overcome where there is a most compelling governmental need. To address the unique concerns in a leak investigation, a federal shield law should require the courts to strike a balance between "the public interest in compelling disclosure, measured by the harm the leak caused," and "the public interest in newsgathering, measured by the leaked information's value."[39]

Establishing such a statutory privilege is not about meeting the needs of reporters; it is about the need of the American people for the information that can only come from confidential sources. Today we often provide more protection against the unmasking of a source who posts anonymously on a website, whose reliability cannot be tested, than to a source who talks confidentially to a reporter, who can verify the information and put it into context before it is published. This should change.

4. Impose safeguards when confidential source and newsgathering information is obtained.

Finally, legislation should impose strict standards about what can be done with the records of a reporter's communications in those very rare circumstances where obtaining them is found to be justified. From the moment that we learned AP phone records had been taken by the Department of Justice, our goal was to prevent any misuse of those records, but there were no legal rules clearly limiting what the Department could do with them. Among other restrictions, the Department in such cases should be required to:

- Disclose to the reporter the type, date range, and quantity of records it has obtained;
- Strictly limit access to the records to those working on the investigation in which they were obtained, and only then on a need to know basis, with no duplicate copies made, circulated or maintained;

---

[39] *In re Grand Jury Subpoena (Judith Miller)*, 438 F.3d at 1162. When Congress a few years back attempted to craft a federal shield law, for example, its legislation provided that the proposed reporters' privilege could be overcome only when "nondisclosure of the [reporter's] information would be contrary to the public interest, taking into account both the public interest in compelling disclosure and the public interest in newsgathering and maintaining a free flow of information." *Free Flow of Information Act*, S. 2035, 110th Congress, Section 2(a)(3) (2007).

- Use the information in the records solely in connection with the investigation and not for any other investigation or purpose;
- Not share the information with any other organization or individual inside or outside of government;
- Other than information admitted at trial, not maintain the information in any searchable database; and
- At the conclusion of any criminal proceeding, keep only one copy of the records (to the extent legally required) maintained in a secure, segregated repository that is not electronically searchable or accessible.

Conclusion

The issues you are considering today are of tremendous importance. The virtues of democracy serve little end if the public does not know how power is being accumulated and when it is being misused. Yet, journalists cannot provide the public with the information needed for democracy to function in a regime where prosecutors can so freely compel the disclosure of journalists' confidential records and information. Given both recent and extensive history, Congressional action is needed to avoid this untenable result.

Thank you for the opportunity to submit these remarks.

About AP

The Associated Press is an independent global news organization dedicated to factual reporting. A non-profit organization founded in 1846, AP today remains the most trusted source of fast, accurate, unbiased news in all formats and the essential provider of the technology and services vital to the news business. More than half the world's population sees AP journalism every day. Online: www.ap.org.

Chair NADLER. The technological landscape has changed dramatically since Congress enacted the Stored Communications Act in 1986.

Mr. Burt, how has the government become more and more reliant on section 2703 electronic surveillance orders since the passage of the Stored Communications Act of 1986?

Mr. BURT. Government has become increasingly reliant on these secrecy orders since that time, and that has been largely the product of the advancement of technology.

At that time, the cloud didn't exist. The substantial extent to which citizens, organizations, corporations, and society in general stores their private communications, their corporate records in the cloud, that didn't exist.

So, today, what we have is a world where access to that information and the application of a secrecy order enables law enforcement to conduct these investigations and get access to citizens', organizations', and corporation records without notice to the organization or the individual whose records are being obtained. That is a dramatic shift in the way law enforcement can and should conduct its operations.

Chair NADLER. Ms. Burton, what are some examples of cases in which you think the government would not need to rely on section 2703 orders but it, in fact, does?

Ms. BURTON. I would point the Committee to the BALCO case, which was a series of stories by the San Francisco Chronicle on sports and steroids, where the government had a two-party process to get information. They were going through the courts, and they didn't like the results they were getting, so they turned around and they went back to the service providers, and they sought the telephone records of the reporters in court without any notice to us. That order is still sealed. We have no knowledge whatsoever what the telephone provider argued in the courtroom.

A perfect example of a relatively routine case. The government was embarrassed about what happened in the grand jury and what came out of the grand jury. It just wasn't necessary. The usual constitutional protections and the courts balancing those and with notice to these reporters was a perfectly fine way to proceed. Whether they won or lost the case, it was fair under a constitutional scheme.

So, there is an example where it was just easier for the government to get what it wanted, and it got it, and it acted in accordance with process that's just not defensible in this country under our aversion to secrecy, as Representative Jordan spoke about when he started with you in this proceeding.

Chair NADLER. Mr. Burt, same question.

Mr. BURT. In addition to the examples that I described in my testimony, let me just offer a very recent example.

We received just yesterday a demand for access to data of a single employee of a major American city in an investigation that has nothing to do with national security. The gag order, therefore, prevents us from notifying anybody in the city—not its mayor, not its city attorney—that an employee of theirs has had their information taken by the government.

More importantly, we also saw with this particular gag order a new trend, or an example of a new trend, a troubling trend that

we're observing, which was, this gag order wasn't just about that subpoena; it was a blanket gag order that purports to cover all subpoenas, all warrants, every process in that entire investigation, in that entire case, all based on one boilerplate submission to a magistrate.

That's the kind of—our law enforcement agents work hard to do a very important job, but the laws that currently exist enables them to act this way out of expediency and convenience, and that's why we need reform.

Chair NADLER. Thank you.

If the recent reporting is true, gag orders prevented counsel within these targeted media companies from sharing any information about the requests for information with the affected reporters. These dynamic strains the attorney-client relationship, to say nothing of its effect on a free press.

Ms. Oberlander, does the Department's use of secrecy orders violate due-process protections? Why do you believe the Department defaults to section 2703 and secrecy orders in this way?

Ms. OBERLANDER. Well, I absolutely believe that it does violate due process. It creates incredible stress for the media organizations and for the lawyers at issue here, the in-house counsel who were aware of the requests but who weren't allowed to tell their bosses, their supervisors, or the journalists or even the newsroom that these requests had been made. It puts them in an incredibly difficult position, as I'm sure, as many of you are members of the bar, you can imagine, when you cannot tell your client crucial information about what is being asked of them and going on.

The other big problem is that, when you have these secret orders, you can't negotiate them. I mean, if the order had come through and the people were allowed to know about it, then they could go back and say, you don't really—even if you want this information, which we don't think you should have, you don't want this other information. We want to make sure that you're not getting other communications that may show our other sources, our other work product, our other confidential investigations.

So, it really makes it very, very difficult for in-house counsel and outside counsel to work effectively with the government and to protect their First Amendment rights.

Chair NADLER. Thank you.

My time has expired.

Mr. Jordan?

Mr. Gaetz?

Mr. GAETZ. We're on a roll, Mr. Chair. Last week, you brought Big Tech to heel; this week, bringing the Department of Justice to heel. My heart flutters to think what might be in our next Committee week. Maybe we'll reform FISA and continue the bipartisan momentum.

I believe that the Department of Justice and the intelligence community shouldn't threaten or spy on Members of Congress, our staff, or the press for politics. President Biden believes the same thing. In response to questions from CNN's Kaitlan Collins, President Biden committed that he would not allow the weaponization of his government against the press.

Chair Nadler agrees. As a matter of fact, Chair Nadler stated, and I'm quoting directly, "Congress must make it extraordinarily difficult, if not impossible, for the Department to spy on the Congress or the news media. We cannot rely on the Department alone to make these changes."

When I saw the reports about Members of Congress's offices being targeted—Mr. Swalwell, Mr. Schiff—I was the first and the only Republican to say that was improper. More of my colleagues should join me.

It was easy to believe that the Department of Justice would do that to the Democrats because they threatened to do it to us.

Mr. Chair, I seek unanimous consent to enter into the record a FOX News publication from September 27th, 2018: "Rosenstein Launched 'Hostile' Attack in May Against Republicans Over Russia Records."

Chair NADLER. Without objection.

[The information follows:]

MR. GAETZ FOR THE RECORD

Print Close

Rosenstein launched 'hostile' attack in May against Republicans over Russia records: congressional email

By Catherine Herridge, ,

Published September 27, 2018

Fox News

Deputy Attorney General Rod Rosenstein initiated a "very personal and very hostile" attack on House Republican lawmakers and staffers in May after they requested records about the FBI's investigative strategy in the Russia case, according to a congressional email documenting the meeting, as well as two additional sources.

The congressional email reviewed by Fox News documented a May 10 meeting at the Justice Department. The meeting reportedly included Rosenstein; his deputy Ed O'Callaghan; senior law enforcement and intelligence officials; House Intelligence Committee Chairman Devin Nunes, R-Calif.; Oversight Committee Chairman Trey Gowdy, R-S.C.; and committee staffers.

On April 24, congressional investigators had sent a classified letter to Attorney General Jeff Sessions and, on April 30, a subpoena for records about alleged surveillance abuse. Rosenstein signed the final surveillance warrant for Trump campaign aide Carter Page in 2017.

"Before the door even closed, we could hear DAG Rosenstein scream at Chairman Nunes, the substance of which we would be briefed on afterwards. The summary is that DAG Rosenstein launched into personal attacks against Nunes, and myself, calling me out by name," Kash Patel, the intelligence committee's national security adviser, wrote. "Demonstrating childish behavior, and a pattern in doing so, the DAG, without facts to support his claims and relying on false media reporting, personally attacked a staffer, myself and our committee."

A source familiar with the closed-door meeting backed up the email account. "Yes, the attacks were very personal and very hostile. Chairman Gowdy tried to calm everyone down and focus on the issues at hand," the source told Fox News. "Deputy Attorney General Rosenstein initiated the confrontation and was much more upset than Chairman Nunes."

A second source who also declined to speak on the record, citing the sensitivity of the incident, supported the account.

However, a Justice Department spokesperson disputed the characterization, saying, "This is not an accurate portrayal of the May 10 meeting as the deputy attorney general, deputy FBI director, and deputy DNI director can attest."

Spokespeople from the oversight and intelligence committees declined comment.

The claims amount to the latest account calling into question Rosenstein's professional conduct while overseeing the inquiry into alleged Russian meddling in the 2016 elections. The New York Times reported last Friday that he had considered secretly recording President Trump in May 2017 and invoking the 25th Amendment to remove him from office after Director James Comey's firing from the FBI. Rosenstein called the Times claims "inaccurate," and a source who was in the room told Fox News the comment was "sarcastic."

Rosenstein, on the heels of that report, had been scheduled to meet Thursday with Trump to discuss the allegations. But that meeting has been rescheduled to next week, the White House said, so as not to conflict with a Senate judiciary hearing on alleged sexual misconduct by Supreme Court nominee Brett Kavanaugh.

Sources said earlier this week that Rosenstein expected to be fired when he attended a Monday meeting at the White House, but Press Secretary Sarah Sanders later said that Trump and Rosenstein spoke by phone and agreed to "sit down and have that further, longer and more extended conversation in person."

Earlier this year, Fox News reported that Rosenstein threatened to "subpoena" emails and other documents from lawmakers and staff on the House intelligence committee during a tense January meeting over the Russia investigation, according to emails documenting the encounter. In that incident as well, aides described a "personal attack."

Those emails, also memorialized for the House general counsel by Patel, described a closed-door meeting involving senior FBI and Justice Department officials, as well as many of the same House members. The account claimed Rosenstein threatened to turn the tables on the committee's inquiries regarding the Russia probe.

When the Fox News story was published in June, a DOJ official said the department and bureau officials in the room were "all quite clear that the characterization of events laid out here is false," adding that Rosenstein was responding to a threat of contempt.

ROSENSTEIN EYEING RESIGNATION, BUT HIS DEPARTURE WOULD CAUSE A FIRESTORM

"The deputy attorney general was making the point — after being threatened with contempt — that as an American citizen charged with the offense of contempt of Congress, he would have the right to defend himself, including requesting production of relevant emails and text messages and calling them as witnesses to demonstrate that their allegations are false," the official said.

"That is why he put them on notice to retain relevant emails and text messages, and he hopes they did so. (We have no process to obtain such records without congressional approval.)"

But during late June congressional testimony, Rosenstein said the incident never happened.

Rep. Jim Jordan, R-Ohio, asked: "Mr. Rosenstein, did you threaten staffers on the House Intelligence Committee? Media reports indicate you did."

"Media reports are mistaken," Rosenstein responded.

Jordan countered by asking whether he'd threatened to subpoena their calls and emails, as alleged.

"No, sir, and there is no way to subpoena phone calls," Rosenstein said.

Print Close

URL

https://www.foxnews.com/politics/rosenstein-launched-hostile-attack-in-may-against-republicans-over-russia-records-congressional-email

Mr. GAETZ. Rosenstein threatened Kash Patel, who was a Member of Republican staff, with criminal process if he did not bend to what Mr. Rosenstein wanted at the time. So, it's not hard to believe.

The most-watched cable news host has been stating for the last several nights that the NSA has been monitoring his communications. Amazingly, the NSA has issued a statement that is so couched it is functionally an admission.

Let's review. The NSA says—on June 28th, 2021, Tucker Carlson alleged that the National Security Agency has been, quote, "monitoring our electronic communications and is planning to leak them in an attempt to take this show off the air," close quote. This allegation is untrue. Which allegation? The statement continues, "Tucker Carlson has never been an intelligence target of the Agency, and the NSA has never had any plans to try to take his program off the air," and the statement continues. What's interesting is that there is no denial that they were monitoring Tucker Carlson even if he wasn't the target.

We saw this exact playbook with Carter Page and Donald Trump, where, to try to assess information from one person, the intelligence community will utilize authorities to go after someone else to try to ensnare their true target. I think that's why they were going after Democrat staff, to try to get to Schiff and Swalwell. I think it's the reason they were going after Republican staff, perhaps to target Mr. Nunes or others. I think it's why they were going after Carter Page, to get to Trump.

I think that there was probably somebody in Tucker Carlson's orbit that NSA was monitoring, and there's no denial that they caught up Tucker Carlson in that monitoring. By the way, there's also no denial that there was a plan to leak the information to try to in some way embarrass Tucker Carlson. The only denial is that they weren't expressly trying to get his show off the air.

It's not like the NSA has never lied to us. I mean, we were told that there was no bulk collection of Americans' data. Turns out, there was bulk collection of Americans' data. No one ever was held to account for that.

The Chair's right or Professor Turley's right, too, we cannot count on these people to police themselves. So, it's my expectation that there needs to be greater review here.

So, Mr. Chair, I am inviting you to continue this bipartisanship. Join me in calling for an inspector general investigation into any monitoring that the NSA or any other element of the intelligence community has engaged in relative to Tucker Carlson. Because these denials, these couched denials, raise more questions than they provide answers.

By the way, if Democrats don't do this, if you're only outraged when your Members and your staff and the press that's close to you and that amplifies your messages is targeted, then we never are going to solve anything. It will, in fact, be déjà vu all over again, as Professor Turley said. I am equally outraged when they target the people I like and the people I don't like, when they target the press that I watch and the press that I despise.

I would greatly seek any bipartisan agreement. Last week, we were on such a roll; we brought Big Tech to account. My hope is

that we can join together again and address this legislatively but specifically with a call for an inspector general investigation into these allegations.

I yield back.

Chair NADLER. The gentleman yields back.

Ms. Lofgren?

Ms. LOFGREN. Thank you, Mr. Chair.

As I listen to these very skilled and knowledgeable Witnesses, it occurs to me we're being asked to provide additional protection to the press because of the First Amendment, but it seems to me our real focus—not that the press doesn't need additional protection under shield laws—ought to be on the Fourth Amendment.

Once again, we are called to ask whether the Fourth Amendment is really still alive in the digital age. The warrant requirements and the guarantees against unreasonable search and seizures really are—they're foundational rights. They're not just to the press, and they're not just to Members of Congress; they're to every American. I do believe that the situation we have here is an end run on the protections that the Fourth Amendment is supposed to provide to every American.

It's true that if the information sought was on a person's desktop, a warrant would have to be issued. There wouldn't be a gag order; there would be notice. The fact that the information is stored in the cloud instead is really meaningless. The expectation of privacy on the part of the individual is that it's their data.

I think we really need to revisit the whole scheme that we have here about Americans' expectation of privacy. When these laws were written, there was no cloud. We ought to extend the Fourth Amendment protections to individuals' data, wherever held, when there is an expectation of privacy.

Now, Mr. Burt, I'd like to ask you about compelling cloud providers, like Microsoft, to produce communication records. The Stored Communications Act allows the government to compel such data upon a showing of reasonable suspicion. Do you think that this standard is sufficient to protect the privacy rights of individuals who have their data stored in your cloud?

Mr. BURT. No, that standard is clearly not sufficient. That's why we're recommending the heightened standard that we do recommend that the Committee consider in legislative reform.

That standard has been turned into these boilerplate approaches that we discussed that enable law enforcement to just simply assert a conclusion that the secrecy order is necessary. Then, as you point out quite accurately, that denies the target of that investigation any opportunity to exercise their Fourth Amendment rights, because they don't know that their property is being taken and searched and seized.

What we've done in our litigation is assert our First Amendment right to inform our customers. While some courts have recognized that we do have a First Amendment right to inform customers—and that's why we also believe part of the reform should clarify that that First Amendment right does exist for cloud providers, because there have been some courts that have found the opposite.

We really need to ensure that citizens have the opportunity to exercise their Fourth Amendment rights. That requires a height-

ened standard. It requires the specific findings of fact that a secrecy order is truly necessary under the existing statutory factors and a record so that only in those very limited instances where it's truly necessary in the national interest is a secrecy order applied, and not 3,500 times a year just to one cloud provider.

Ms. LOFGREN. Right now, the entire burden of protecting Fourth Amendment rights falls upon the service provider. Now, I heard your testimony that Microsoft is active in protecting those rights, but there are other providers that may not be active. The fact is, it's the individual whose rights are being challenged who should have the opportunity to contend and to protect.

I would like to think, what happens when a court issues a secrecy order that later turns out to be totally unsupported and yet the government uses the information it gets in the request to bring a criminal prosecution? Can the defendant use the secrecy order as a basis for suppression? Do you know that?

Mr. BURT. I would yield to Witness Mr. Turley to see if he's got a specific analysis of that. I believe the answer is, there is no opportunity for the defendant then to challenge the evidence that's seized in that way under a secrecy order under the Fourth Amendment.

Chair NADLER. The time of the gentlelady has expired.

Mr. Biggs?

Mr. BIGGS. Thank you, Mr. Chair. Thanks to you for holding this very important hearing, and thanks to the Witnesses for being here today.

I associate myself with basically everything that's been said here today. It's been remarkably agreeable, which is really pleasant and surprising. I hope that we can work together to try to bring clarity and rectification of these problems.

So, here's my first question goes to Ms. Burton, this is for you. You said in your written report, because information's in the cloud storage bin rather than in a file cabinet—and, by the way, this was iterated by every Witness—the government should have no greater investigative and secrecy interest due to the case—due to the ease of access.

So, I guess my question is, if you were the DOJ or government, how would you respond to that? Because, I mean, that's the blankest statement, is that there is no greater—just because it's easier to claim secrecy, there's no greater case for it. How would you respond if you were DOJ to that?

Ms. BURTON. I mean, if I were the Attorney General—and I think he's headed in this direction—I would want to be responsible, as a citizen of the country, to balance all rights and all needs.

That's why we have judges. That's why we have notice. That's why we should not be putting our cloud providers, effectively, above the Constitution. As you say, Microsoft makes some efforts in this regard, but that is it not universally the issue.

I would tell you, there's a lot of things we don't know right now. If I'm the DOJ, I don't want to be convicting people or bringing cases where I can't defend in full measure the evidence that I put before a court and give someone the right to challenge that. I think that's just playing, should we say, pro ball in a bad way.

Mr. BIGGS. Well, I don't disagree, but I haven't heard, basically, from any of the Witnesses, nor have we seen in practice over years, that DOJ really is concerned with being a pristinely good, due-process adherence, and protecting the rights of everybody. I mean, you've all iterated examples where they've abused this authority.

Mr. Burt, this is coming into your shop 3,500 times a year, and so we're led to believe that this could be many thousands of times.

So, you've given your set of prescriptions as well, but why do you think it should be—on a physical warrant, with physical materials being seized, it's a 30-day—if it's going to be secret, it's 30 days per statute. Why do you think it should be 90 days for data?

Mr. BURT. That's a very good question. Any reasonable time is acceptable to us and to the technology industry. What we're trying to do is rein in what we have seen, which are indefinite secrecy orders that have no termination date.

What we've seen since the DOJ formulated its policy in response to litigation, we filed back in 2017, we've actually seen somewhat of a decrease in those indefinite orders, but we still get hundreds of every year. The standard that we see, typically, is a year. That's just far too long a time period, even when it's actually justified to have a secrecy order.

So, our response would be, there's a very small universe of truly justified secrecy orders. Where those secrecy orders are truly justified, then as long as 90 days might actually be acceptable.

Mr. BIGGS. I just have just about a minute left, and I would like each of you to respond to this. Because each of you have talked about, one way or another, reliance on the courts as arbiters here, and yet they seem to be just rubber-stamping boilerplate language.

I am concerned about what I view as a necessary stick approach to DOJ for their abuse. What is an appropriate punitive measure?

I mean, in a regular criminal case with physical evidence, you're going to have the exclusionary issues that will come in if there's fruit of the poisonous tree, et cetera. What happens here? What is the punitive measure that devolves to bad actors, DOJ?

Professor Turley, we'll go with you and then right down the table.

Mr. TURLEY. Well, I certainly agree with your point that the courts have not exactly covered themselves in glory. Part of the problem here is that these judges are getting thousands of these things, and they don't want to go into the weeds on some of these issues.

So, you have cases like In re Grand Jury out of the ED New York that are saying, look, this is boilerplate, we are just getting boilerplate over and over again, and that's not saying anything.

You're going to have to structure what a court has to find and what a court must establish in writing if we're going to be able do anything. I think you have to establish standing in an appellate procedure with adversarial process. Those are the things that will result in a change.

Chair NADLER. The gentleman's time has expired.

Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chair, thank you so very much.

I view this as enormously crucial in holding this bipartisan hearing, and it gives me reflections down memory lane of the Patriotic

Act and the urgency after 9/11 to deal with both, as we fought for in the Judiciary Committee, the balance of civil liberties, as well as this major effort to be able to protect America.

We've come full circle, I believe, and we are here to protect America again. We're doing it from a different perspective.

Allow me just to lay a predicate, if I might, that under the Trump Administration's Justice Department they sought the phone and email records of journalists, Members of Congress, their families, and their staff. I think we should just dwell for a moment: Staff and families.

Now, I imagine there's an array of family members and there might be a toddler. Some said there was a child whose various resources were sought as well.

Donald Trump's determination to repeat the abuses of President Nixon was carried out in his contempt for the invaluable service to democracy performed by a free and independent press, his desire to punish politicians who opposed or criticized his policies and actions.

As I pointed out during the impeachment proceedings against Donald Trump, his conduct reflects and reveals a person whose character is thus marked by every act which may define a tyrant and shows he is unfit to be the ruler of a free people.

I say that for the record, not to suggest that what we're doing today should appeal or apply, appeal to all of us and apply to all of us regardless of our political perspective, as I heard Witnesses say.

In fact, Ms. Oberlander, you indicated, if sunshine is the best disinfectant, it is obvious that this shadowy State of affairs allows for all manner of dark things to grow.

We worked very hard in the PATRIOT Act to pull back, dealt with Pfizer. Even in our effort to do so we have had our ups and downs.

So, let me ask all of you a question. It is just a yes or no to all the Witnesses. Then, with the time remaining, I'll ask a specific question. Let me start.

Professor Turley, do you believe that Congress definitively needs to act in the midst of what we're dealing with at this time?

Mr. TURLEY. Yes.

Ms. JACKSON LEE. Mr. Burt?

Mr. BURT. Yes, I do.

Ms. JACKSON LEE. Ms. Oberlander?

Ms. OBERLANDER. Yes, I do.

Ms. JACKSON LEE. I believe Ms. Burton?

Ms. BURTON. Yes, ma'am.

Ms. JACKSON LEE. Thank you.

So, let me pose this question to Ms. Burton.

How might the use of electronic surveillance gag orders used to further a President's personal crusade, what impact do you think that has as relates to the industry?

Ms. BURTON. I would say, Representative, that what you need to do in our answer to yes, and how it would affect not just the industry of the media, because I think what we have really determined here is that this affects all Americans.

So, I would urge you to put forth legislation that would have a foundational matrix that could apply to the First Amendment, the Fourth Amendment, a narrow statute that covers broad constitutional considerations. That would be to give notice, due process standards, courts, judges, and no secrecy.

I think that combination of things in a narrowly stated, not all the other issues that we've touched about on a lot of issues, but something very simple and clear that would effectively help our industry and the American public to no end.

Ms. JACKSON LEE. Thank you, Ms. Oberlander.

Let me ask you the question from the reverse.

What should be the limitations on our effort to protect the American public against these random securing of data now in the light of the cloud? Should there be from, your perspective, the First Amendment specialists, what limitation should we consider, if any?

Ms. OBERLANDER. Congresswoman, I think that, frankly, the protection for the media should be broad and it should be subject to strict judicial review any time you're trying to get—government is trying to get this material to invade the privacy of the journalists, to invade the privacy of the reporting process.

It may be that there are specific places where you could override that, perhaps on acts of terrorism, obviously, if there is a reason to believe that there's communications around terrorism or the identity of the terrorist. That might be one of the places where you would have a narrow exception. I do think it is—or imminent bodily harm, or violence, or immediate death.

In general, I think the protection should be very, very broad and subject to independent judicial review. As the other Witnesses have said, there should also be the right of interlocutory appeal for that.

Chair NADLER. The time of the gentlelady has expired.

Ms. JACKSON LEE. Thank you. I yield back.

Chair NADLER. Mr. McClintock.

Mr. MCCLINTOCK. Thank you, Mr. Chair.

I find myself in complete agreement with Ms. Lofgren. This is not a matter of special protections for journalists or public officials. This is a matter of the Fourth Amendment right of every American citizen.

It was John Adams, who was certainly in a position to know, who said that in his opinion the American Revolution started many, many years before 1776 with the King's abuse of general warrants. That's when he said the "Child Liberty" was born. We wrote our Fourth Amendment to assure that such abuses could never threaten Americans.

Professor Turley, I am not an attorney, but perhaps you could give me a little bit of schooling.

It is my understanding that if the government wants to go through my papers to search for a document, an incriminating document, it first has to go to a judge, convince that judge there is probable cause to believe that I have committed a crime, and that the evidence for that crime is likely to be found among my papers.

Do I have that correct?

Mr. TURLEY. That is correct. They have to satisfy the standard of probable cause.

Mr. MCCLINTOCK. So, does it make a difference if that paper they are looking for is in my safe deposit box at my bank?

Mr. TURLEY. No. That's the oddity about this situation, is that because of this new technology and storing on the cloud, suddenly a large amount of your information has become vulnerable to being seized.

Mr. MCCLINTOCK. Why would that make any difference? It could be seized sitting in my safe deposit box, but they can't just go and seize it. They have to first abide by the protections afforded me under the Fourth Amendment. Is that correct?

Mr. TURLEY. It shouldn't. What they are getting thorough metadata and other types of searches is a great deal of information that people would believe is private.

Mr. MCCLINTOCK. My point is, whether I wrote those incriminating words on a piece of paper or wrote them digitally, it's the same thing exactly. Whether I store them at home or in a safe deposit box in the case of a paper or on somebody's server in the case of the cloud, it makes no difference, it is the same thing.

Mr. TURLEY. That's right. What's particularly bizarre here is that the most famous case of the Supreme Court in the privacy area is Katz, where the court said that the Fourth Amendment protects people, not places. Yet we have the ultimate rejection of Katz because if you move information from one place to another it suddenly moves out of a warrant and probable cause protection.

Mr. MCCLINTOCK. How have we allowed ourselves to get so far from these fundamental Fourth Amendment principles that underpin our liberty?

Mr. TURLEY. It's really two things. One is the court opened us up for this when it decided in cases like *Smith* v. *Maryland* that pen registers don't require warrants. A lot of that is based on a myth. The Court said, well, you give your phone number to a third party, i.e., the telephone company.

Well, it used to be a human being there putting in your phone number. Now, of course, you are giving it to a computer. So, people are not giving their information to a third party knowingly. The Court has never corrected that misunderstanding, in my view, of the privacy dimension.

The other aspect to this is just new technology. We have constantly seen privacy protections that have failed with new technology. This age we're living in is making a mockery out of the standards created by the court.

Mr. MCCLINTOCK. The technology may change, but human nature doesn't change and the principles that undergird our Constitution don't change because they are rooted in human nature.

Mr. TURLEY. Mr. McClintock, I also want to note that there's a growing gap because the court just decided in Carpenter that you need a probable cause determination and a warrant to get the location off people's cell phone. All of us celebrated that as a victory of the Fourth Amendment. Yet, you don't need a warrant to get information from the cloud. From a privacy perspective, this is not just nonsensical, it's dangerous.

Mr. MCCLINTOCK. Yeah. Well, I just wonder, how are secret courts and secret subpoenas and secret letters compatible with a free society? Can a free society exist if its government can secretly

surveil its citizens in this manner in direct contravention of its most fundamental law?

Mr. TURLEY. Yeah. One of the great dangers, by the way, Katz had within it seeds of its own destruction, because it bases the test of privacy on our reasonable expectations of privacy. So, as our expectations fall, the government's ability to engage in warrantless surveillance increases, and that could become this race to the bottom.

Mr. MCCLINTOCK. They say this is necessary for our national security, for our country. The only oath that any public official takes is not to support and defend the country, not to support and defend the government, it is to support and defend the Constitution. There's a reason for that. Our Founders understood if we ever lose our Constitution, we've already lost our country.

Chair NADLER. The time of the gentleman has expired.

Mr. Cohen.

Mr. COHEN. Thank you, sir. Thank you, Mr. Chair.

Most of the questions I think have been asked that are pertinent but let me ask this? I'm not sure if this is to the right person, because we probably should have the Justice Department before us, as well to let us know what's been going on.

Ms. Oberlander, do you know of any cases, or do you have reason to believe there are other cases that have not been reported where there has been surveillance that would concern the American public and this Committee?

Ms. OBERLANDER. I don't actually have any direct knowledge of any cases that haven't been reported. I would imagine that there are. We have just learned about a significant number of attempts to find out the information of various journalists and various other Members of the Congress. I don't have any direct knowledge of that, though.

Mr. COHEN. Ms. Oberlander, you're a representative of the, I guess, the Fourth Estate, the press, and they are protected by the First Amendment. We as Congress people are concerned about Article I.

The public, as Mr. McClintock and Ms. Lofgren have discussed, they are the subject we most need to be concerned about.

Do you have any—what are your suspicions on what type of cases and what people have been spied upon through this means?

Ms. OBERLANDER. Outside of journalists?

Mr. COHEN. Outside of journalists.

Ms. OBERLANDER. Actually, honestly, really, I am a representative of the Fourth Estate here and I am unaware of whoever else may or may not have been spied upon outside of the media.

Mr. COHEN. Well, thank you.

Mr. Turley, I think you've discussed some of the exceptions that might be made if we had a law, and I don't know who it was addressed to, that we should have—they should all be warrants and they should be somehow adversary hearings and appealable to some higher-level court.

Are there other suggestions that would you make to protect the public in these circumstances?

Mr. TURLEY. My testimony actually does contain some initial suggestions.

It's very important to address the standing issue. We've had cases in which people, particularly media, have tried to get this issue into court and they've just been told, "You don't have standing," which is completely bizarre, because this goes directly to who the media is and trying to protect their constitutional function.

There are also limitations on appeal that you can look at.

I think you can also in drafting language create more of a legislative presumption that applies in these cases to make it clear to courts that the default position should be not to have a gag order, the default position should be not to have these secrecy issues.

To give you an example, the important thing here is remember that prosecutors are rational actors. Many are my good friends; I litigate against them. They are rational actors, and they follow the path of least resistance.

If you look, for example, at studies with the national security letters, from 2000–2005 the number of national security letters went from 8,500–47,000.

Now, you only have that exponential growth if it is the path of least resistance. You have to make that path a little more difficult.

Mr. COHEN. Well, I agree with you. We need to make it more difficult, and we need to protect the citizens.

What concerns me—and I think we're going have a briefing from the Justice Department after the break—is when did they know, the new team, and what do they know about these intrusions on the Congress and the press and the gag orders?

Did they only come to the public's attention after *The New York Times* had reported them? If so, if they had knowledge beforehand and waited, didn't plan to make this public, then I've got concerns.

I think that I have faith in Merrick Garland, I have faith that he will change the Justice Department's personnel to get it to be more transparent. It would be disturbing to think that they had this information and only but for *The New York Times* reportage was this forthcoming to the public about the intrusion into Mr. Schiff and Mr. Swalwell and everybody else's—and the reporters'—otherwise, private communications.

So, I think we've got to go further, but we do need to draft legislation that protects the public, that does put this in front of a court.

Professor Turley, do you think there ought to be—is there just one court that issues these or are there many courts?

Mr. TURLEY. I think you can still—the problem is that the sheer number of these cases is just breathtaking. So, if you pour all these into a single court, you're going to have a massive court. Judges can handle these questions, but they need more structure from you.

I also want to echo; I have faith as well in Attorney General Garland. In fact, I think that he is ideal to deal with this question because he's walked the walked. He's been a judge. He's dealt with these types of docket issue. He is now at the head of the Justice Department. I think that he could be a really terrific ally if he means what he says, and we can try to solve this problem.

In the past, the Justice Departments has not been a faithful ally, I must tell you. Fifteen years ago, we talked about this, and the Justice Department was opposed to shield laws and a lot of these provisions.

I do have faith in General Garland. I am hoping that faith is well established.

Chair NADLER. The time of the gentleman has expired.

Mr. Massie.

Mr. COHEN. In my last [inaudible], Mr. Chair, I would just like to say to Professor Turley, the last time we had contact I was a little brusque maybe with you, a little rough shoulders. You're a gentleman and a scholar. I appreciate you. I apologize if I want too far.

Mr. TURLEY. Thank you very much, Representative.

Chair NADLER. Mr. Massie.

Mr. COHEN. You're welcome.

Mr. MASSIE. Thank you, Mr. Chair.

I would like to associate myself with the comments from Mr. McClintock and Ms. Lofgren that any protections that we provide shouldn't be for a special privileged group of people. I mean, that's not the way the Constitution was written.

Ms. Oberlander referred to the press as the Fourth Estate, which prompted me to look up what are the other three estates. It's a reference actually not to the three branches of government, but to the three estates in Europe, which were the clergy, the nobility, and the commoners.

I think all of them, including the Fourth Estate, deserve the protections of the Fourth Amendment. So, whatever we draft, I hope it is not just particularly for Congress or for the media.

Professor Turley, you touched on something earlier but didn't get to spend enough time on it, about the third-party doctrine. Can you explain to us in a little more detail how that came about and what we could do in Congress to sort of rein that back in?

Mr. TURLEY. Yeah. Quite frankly, I think the Supreme Court has made an utter mess of this area. I think even people like the late Justice Scalia made reference to the fact that constitutional criminal procedure, which I used to teach, was just an absolute morass created by the Supreme Court.

Part of the problem is this idea of third parties, that if you give things to third parties you don't have that same expectation. They treat things like pen registers, giving phone numbers, almost as equivalent of, like Greenwood, of putting your trash on the curb, that you give up all expectations of privacy because you're giving it to someone that you don't know.

Of course, when people put in phone numbers, they are giving it to a computer that they assume is subject to some types of regulation.

That has gradually expanded where the exceptions are now the rule. So, you have with cases like *Smith* v. *Maryland* a lower standard than probable cause under the warrant clause.

What you have to understand is every time the court creates one of these exceptions' prosecutors pour into the gap. It is not because they are little petty tyrants, it is because they have a lot of cases, and they believe very strongly in getting information. They want to get it fast.

That's why you've had this massive increase in national security letters because it's so much easier. You virtually have to show nothing.

So, it's going to be up to the Congress to make that path a little more difficult, to require showings. The most important thing is to have some adversarial process and standing so that people like us can come and challenge these things.

I do classified work in the national security area, and I'm read into programs so that the judge and the cleared prosecutor and I can argue about evidence. Those are the most extreme possible cases you can imagine. Some of those cases are really classified at the highest level.

This should not be so difficult, because this is not highly classified information in the vast majority of these cases.

What I think you heard from Mr. Burt is very important. I mean, his company is getting 3,500 requests a year.

Mr. MASSIE. Shouldn't the analogy, instead of being taking your trash out to the corner and leaving it there, treating your data that way, shouldn't it be more like a safe deposit box?

If I put something in the cloud, I have an expectation that you're going to do your best effort to keep it private. Yet, we've turned the third-party doctrine, which we somehow are still clinging to, is turn that on its head. I hope we do take that on.

I would just throw out a couple ideas here.

If we were really, really, really serious, we would pass a law that has criminal penalties for those who invade your privacy at the DOJ, FBI, and NSA. I don't care if it is just a $50 fine and 30 days paid leave, whatever it is, if there was some crime associated with doing this. Now, the penalty should be much stiffer than that, obviously.

So, that's one thing I think we would do. The other thing I think we could do is to legalize technical solutions to privacy.

It's technically illegal to make a phone call from a location that can't be determined by the government to a location that can't be determined by the government. Why is that?

It is technically illegal to have encryption that the government doesn't have a key to. Why is that? Why are we outlawing the technical solutions to this problem.

I mean, we're afraid of privacy, but we're clinging to this notion that we can give all the keys to these things to some folks and not supervise them and trust that they won't be rifling through our stuff.

So, those are just a couple of suggestions.

Mr. Burt, I like your suggestion of making sure that all the national security letters or the secret requests are not indefinitely kept secret, but eventually we know about those. That's just critical. We've got to know what we've trying to legislate.

Thank you. I yield back.

Chair NADLER. The gentleman yields back.

Mr. Johnson.

Mr. JOHNSON of Georgia. Thank you, Mr. Chair, for holding this very important hearing.

We are here today because the Department of Justice has come up short. Recent reports document that in 2020 the Trump Administration secretly obtained from third-party platforms the phone and email records of reporters.

This is not the first time or the first Administration under which the Department has done so. We've heard testimony today that DOJ has routinely misused secrecy orders to avoid basic due process protections in criminal prosecutions.

As a country, we've watched Presidents as far back as Nixon use the legal system to aggressively pursue the sources of information and leaks.

Ms. Oberlander, what changes should the current Administration take to ensure that it does not allow its Department of Justice to overreach in terms of secrecy orders and destroying the ability of the Fourth Estate to do its job, which is to maintain our democracy through free and fair sharing of information that is sometimes critical of government?

Ms. OBERLANDER. Thank you, Congressman.

So, first, I do think it is a great idea to, as Attorney General Garland has said, to basically legislate, to work to legislate that the Department of Justice is no longer permitted to come after journalists' source information. I think that would be fantastic.

Short of that, I think you should legislate particular higher standards before the Department of Justice can get access to journalists' materials.

Specifically, there should be—and it should be, again, as people have said, not up to the Department of Justice itself, but it should have to come to an Article III Judge and they should show that the information is absolutely crucial to whatever investigation there is, that they have tried all alternative sources to get that same information and have failed.

There should also be a balancing test by the judge as to whether the information is important enough to outweigh the incredible ability of the press to inform the public about issues of public importance.

So, essentially it is a very high standard. The judge should have to consider that. Then, as we talked about, the media should be able to have notice of it, to be able to participate in it, to argue about it. It should be adversarial and there should be a right of appeal.

I mean, these are very, very serious rights that are being—and they should be subject to judicial review. That would go a long way, frankly.

Mr. JOHNSON of Georgia. Okay. Do you believe that the Trump Administration followed the Department of Justice guidelines when pursuing journalists' sources in the cases of CNN, *The New York Times*, and *The Washington Post* that were recently revealed?

Ms. OBERLANDER. Well, the Department has said that they did follow the guidelines. We don't know. There's a lot of information we don't know. We don't know what information they put before the court in their warrant applications, in the applications before the court to get this information. We'd like to see that.

We'd like to see why a secrecy order was necessary. As I mentioned, these were records that are years old that they were looking for in public—leak investigations that had already been made public.

So, there was no real, at least to my perspective, there was no real risk that having a notice go to the media would have in any

way tipped off the subjects of the investigation or allowed anyone to destroy the evidence.

Furthermore, this material was, in fact, in the possession of the third-party data provider. It wasn't even in the possession really of the media entity. So, the idea that they could then turn around and destroy it is somewhat—doesn't actually make any sense.

Mr. JOHNSON of Georgia. The length of the gag orders in these cases was quite excessive. Would you agree?

Ms. OBERLANDER. I would.

Mr. JOHNSON of Georgia. I mean, two years—

Chair NADLER. The gentleman's time has expired.

Mr. Bishop.

Mr. BISHOP. Thank you, Mr. Chair.

Mr. Burt, I think it bears repeating something that Professor Turley referred to in your testimony, that "Microsoft reviewed the number of secrecy orders that Federal law enforcement agencies have presented to us from 2016 to the present. We found that while the number has increased some, Federal law enforcement has consistently presented us with 2,400–3,500 secrecy orders each year, or 7–10 per day."

Is that correct?

Mr. BURT. Yes, that's correct.

Mr. BISHOP. That's an amazing number, particularly when you try to imagine what that might be when you go to the other big tech firms.

Professor Turley, you have a figure—and forgive me for this ignorance—but you have a figure in your testimony, and you mentioned that the national security letters have gone from 2000–2005, I believe it was, it went from 8,500–47,000 per year?

Mr. TURLEY. That's correct.

Mr. BISHOP. Now, here's my ignorance.

Would the secrecy order, Mr. Burt, that you're describing be the same? Would that include or overlap with national security letters?

Mr. BURT. No, Representative. It would be in addition to.

Mr. BISHOP. So that would be separate, right? So, in other words, a national security letter sort of does similar—there are similar concerns associated with that. That would be over and above what you are talking about, secrecy orders in connection with search warrants.

Mr. BURT. That's absolutely right.

Mr. BISHOP. Are those data published in the aggregate that you know about? Do you understand what I'm asking, Mr. Burt?

Mr. BURT. Yes. The answer is there isn't any reliable source of that information in the aggregate. In fact, with regard to national security letters, we had to sue the government to be able to say anything about that.

The resolution of that was that we can only describe the number of national security letters we get in these broad categories. For example, I can report that—and we do transparently report—that in the last reporting period, twice a year, we got between zero and 499. That's the most specific we can be.

Mr. BISHOP. Fascinating.

Professor Turley, you spoke about in your testimony—I am afraid I didn't get your testimony before the hearing, so I haven't had oc-

casion to digest it—but you advocate for a shield law. You mentioned one that's drafted. You said that it needs to have the definition of journalist modified. As I skimmed through, it looks like you think there needs to be a broader definition of journalist.

This sort of goes to some of what Mr. Gaetz was saying, and I think Mr. McClintock responded to, about the possibility of setting up special privileges for an elite class.

If journalists are partisan instruments of politicians—or the reverse, that is, they direct politicians, in effect—if we establish special privileges for them to be able to take information and disseminate it that is by law confidential, doesn't that grant the power to unilaterally not nullify a law?

If you take the ProPublica information recently, the disclosure of thousands of wealthy taxpayers, selectively published, they said they thought about it, they know this information is unlawful to publish, but they've decided that their advocacy interests trump the law.

How do we deal with that problem?

Mr. TURLEY. Well, this isn't an absolute right. I mean, the media is subject, for example, to defamation, they're subject to being prosecuted for crimes committed directly by reporters.

What we're talking about is a constitutionally founded privilege. In the critical case of Branzburg, the court heavily fractured over this question of privilege. There were some, like Douglas, who always believed we should have absolute privilege. A number of the Justices felt we should have a qualified privilege. In fact, most of the qualified privilege statutes are based on the language out of that case.

A qualified privilege just simply gives some added scrutiny and protection to the media. It can be overcome in extreme cases. It's there to protect this core function of the media.

If you take a look at the States, there's 40 States with these privileges. They haven't shut down prosecution. It has not been overwhelmingly burdensome. The judges have been able to use them. I think the same would happen with the Federal system as well.

Mr. BISHOP. In the 40 seconds I have got left, can you characterize, what is the privilege, what are they privileged to do? What are the qualifications upon that or conditions?

Mr. TURLEY. Well, what the privilege does is it basically gives a full stop for the court. Before you allow reporters to be compelled to turn over information, you have to establish that you can't reasonably get the information from another source, that you have a clear need for this information, where the court's going to balance these interests.

Some of these State laws are quite interesting. In New York, they have a different standard. If you go for privilege, sort of core news stuff, you have an absolute privilege. If you go for less key material, you have a qualified privilege.

There's a lot of States that have explored different types of approaches to this and it gives you a lot of models to look at.

Mr. BISHOP. Thank you, Mr. Chair.

Chair NADLER. The gentleman's time has expired.

Mr. Cicilline.

Mr. CICILLINE. Thank you, Mr. Chair.

I think it's safe to say that all of us were very upset when we read the reports detailing how in former President Trump's Administration the Department of Justice surveilled not only journalists, not only Members of Congress, including a Member of this Committee, but even Members' staff and family.

So, I thank you for holding this hearing today and giving us an opportunity to really look at the potential abuse of power, and particularly the secrecy surrounding these efforts.

I want to first say I agree with Ms. Oberlander. I think there is a higher standard that ought to apply to the press. I think that is reflected in the Free Flow of Information Act that Congressman Raskin has introduced. It has always been bipartisan.

I also think making sure this applies, these protections apply to everyone is important, as Mr. Massie and Ms. Lofgren have said.

One easy way to accomplish it, of course, would be to say the Fourth Amendment applies to the data that you generate, that you have a reasonable expectation of privacy of what you create, and all the Fourth Amendment rights would attach to that.

What I want to focus on in my questions is the secrecy surrounding this, because while Microsoft is an example of a company that takes this responsibility seriously, to litigate it and challenge this, we have no assurances other companies do the same.

Many of these big technology platforms don't have competitors. So, if they are willy-nilly giving your stuff away without contesting it, we don't know about it and we can't choose to go to another platform, because they don't exist. They are monopolies.

So, I want to really dig down on the secrecy, because I think that's really one of the important issues here. I think we don't have a full understanding of what's presented to a court and what the court has to consider allowing these gag orders to be put in place.

So, I am going to begin with you, Mr. Burt.

What level of details are prosecutors required to provide both the court and the providers when they are seeking a gag order? Do they simply have to say, "We meet the statute," or do they have to present facts which show, in fact, disclosure would result in one of the things articulated in the statute?

Mr. BURT. It's a great question, Representative. The answer is that today they only have to present to the court this boilerplate assertion that they meet the criteria of the statute and that there's a reasonable suspicion that they can meet that standard.

Mr. CICILLINE. No facts underlying that assertion?

Mr. BURT. That's right. The Justice Department's policy that they articulated in 2017 in response to our litigation said that they should articulate those facts.

Mr. CICILLINE. Thank you.

Mr. BURT. Their own—

Mr. CICILLINE. No, I appreciate that.

Mr. BURT. Their template says they don't have to.

Mr. CICILLINE. Thank you.

Ms. Burton, what about after the secrecy order is lifted and the provider is able to give notice, how much information is shared with the targeted party? Is it required that the information be shared once the secrecy order has lifted?

Ms. BURTON. No, it's not, Congressman. That's one of the problems. I mean, it's an entirely self-regulated process at the Department of Justice.

To take your concerns, I agree with you. It is not just a First Estate concern, and it is really a self-regulation concern. You cannot have the Department of Justice being prosecutor, judge, and jury. They determine when you get notice, they determine what you know, and you go to an Article III Court and you may or may not have enough information.

Which is why I think you all are very much on the right track to have a procedural set of requirements that are in a statute, that it can apply more broadly, and we leave it to judges, who now have a standard, and there's notice to the parties, and it's not secret.

We don't allow prior restraint in this country of the press. It should not be—

Mr. CICILLINE. I'm trying to get in a couple of questions. I appreciate that. Thank you.

Mr. Burt, once the electronic surveillance-related gag order expires, is there currently an obligation for the Department of Justice to at least notify the target of the warrant that a gag order was in place?

Mr. BURT. Absolutely not. In fact, they don't typically do that, and so it falls upon us do that.

Mr. CICILLINE. That burden that falls entirely on you, are you required to notify your clients or users or does that vary on a contractual basis?

Mr. BURT. We are not required to, but we have a firm policy that we do notify in all cases.

Mr. CICILLINE. Is that same policy in place, to your knowledge, with respect to all the other large technology platforms?

Mr. BURT. To my knowledge, that policy is not in place with all technology platforms.

Mr. CICILLINE. What limited information should the government communicate to suspects, in your view, that their Fourth Amendment rights may have been implicated by one of these orders or collections?

Mr. BURT. Well, we believe that in those very rare instances where this kind of a secrecy order is justified—and we think the standard should be probable cause, facts should be presented, courts should find that the facts are sufficient—but in those rare instances where that standard is met, then when the gag order expires, the target should be informed that there was a gag order and should be informed of the scope of the search.

Mr. CICILLINE. Thank you very much.

Again, it seems to me it is inappropriate for us to expect that third parties are going to fiercely defend the privacy rights of individuals, which this current architecture requires some companies take it seriously, some don't, but citizens and users lose as a result.

I thank you again for your testimony.

I yield back, Mr. Chair.

Chair NADLER. The gentleman yields back.

Ms. Spartz.

Ms. SPARTZ. Thank you, Mr. Chair.

I'm actually kind of listening to all this discussion very surprised how many loopholes our laws have and very surprised to hear our Constitution hasn't changed, thank God. Ultimately, what Mr. McClintock brought up, what's happening, it is really appalling to me. No wonder our citizens are not trusting government and it's very bad.

So, I have a quick question. I think Congressman Biggs brought another good question of rubber stamping. I will yield to him in a second, because I would like to finish that conversation.

Professor Turley, just for you, what allowed for us to have these loopholes? Is it interpretation of the courts? Or is it really something in legal framework that's so ambiguous that we need to clarify? What is allowed?

Because it seems like this due process should exist regardless of if we have a new technology or old technology, where we are. What's happened?

Mr. TURLEY. Well, it's a perfect storm, because you have the court that opened this up creating a whole group of body of searches that can occur below the probable cause level with reasonable suspicion. That snowballed within a short time. They viewed those as narrow exceptions. It became the exception that swallowed the rule.

Then you had technology that poured into that gap. That is, it happened to be technology that fell in those areas. Suddenly we're not protecting people, we're protecting places, or in this case we're not protecting places like the cloud.

So, if you take stuff from one source to another, it's protected over here. The minute it goes to a cloud, which you have to use in many cases, or you use as a matter of course, it loses that protection.

I think your point is really the vital one. I think a lot of people would be very surprised when they find out that their information is so readily available to the government.

That itself is a very corrupting aspect in a free society, that the public has a different view of what their privacy is from what the government is actively doing, not in a small number of cases, in massive numbers of cases.

Ms. SPARTZ. That sounds more like a surveillance State. We have to deal with that. You believe it needs to have some legal actions from Congress to be able to remedy this situation?

Mr. TURLEY. This is not a particularly difficult problem to solve. It only takes will. You can easily create a framework that will protect privacy and fill this gap.

Ms. SPARTZ. Well, thank you very much.

I yield to Mr. Biggs.

Mr. BIGGS. I thank the gentlelady for yielding.

When we left off, when I ran out of time, Professor Turley just answered my question. I'll just remind you of what it is and give you the context.

I was asking about the stick that might be necessary to help what we typically would think of as an independent court.

So, you all seem to be in agreement with guidelines, et cetera, statutory guidelines. How do you make sure that those are going to be tough enough?

Mr. BURT. If I may—

Mr. BIGGS. Yes, Mr. Burt, and then down the line, then Ms. Burton.

Mr. BURT. If I may, I think the concept of extending the Fourth Amendment to data that is stored in the cloud is a reasonable framework to consider here, because then that would take all the existing sticks, as you put it, that would apply when government overreaches and violates Fourth Amendment rights, exclusion of evidence and so forth. It would be applicable here as well.

The irony is that Fourth Amendment jurisprudence is based on this notion of reasonable expectation of privacy. In fact, your security and privacy of your data is higher in the cloud than it would be if you kept it in your premises or on your network at your corporation.

So, the law has not advanced with the technology to protect our citizens and our organizations' information.

Mr. BIGGS. Thank you.

Ms. OBERLANDER. Just to add what my colleague here said, one of the reasons that media organizations are putting their data in the cloud is because they are also concerned about the security and that they can't afford to have the kind of technologies and technologists in their shops, in their shops who could protect from hacking and phishing and all the other problems that we have with our data. So, it puts them in a—puts many of the media companies in a really tricky position.

To the point about what kind of penalties you could have, there is the possibility perhaps of a 1983 action if rights were violated, and journalists have used that successfully in certain cases.

Mr. BIGGS. Ms. Burton, before you answer this, I think we all would presume, at least I do anyway, that there is a private property interest. You have private property rights in your data, right?

It begs the question that Mr. McClintock and Ms. Spartz were raising, and actually Ms. Lofgren, and then Professor Turley expounded on it. Why then do we have these loopholes that attack Fourth Amendment rights over your otherwise well-known, and it should be established, private property interest in your data?

Chair NADLER. The time has expired. The Witness may answer the question.

Mr. TURLEY. If it's to me, the answer—

Mr. BIGGS. Ms. Burton.

Mr. TURLEY. Oh, Ms. Burton. I'm sorry.

Ms. BURTON. I think that the minute we get enough process into a statute that you're going to see prosecutors act more rationally. I would leave it to the courts to suppress the evidence and to dismiss cases. I think that, from a prosecutor's point of view, is remedy enough.

I'm not in favor of creating lots more causes of actions around this. I think we're trying to simplify it. I think we're trying to protect rights. I think the courts would actually make sure that occurred.

Chair NADLER. The gentleman yields back.

Mr. Lieu.

Mr. LIEU. Thank you, Chair Nadler, for holding this important hearing.

Professor Turley, I'd like to follow up on Congressman McClintock's line of questioning and just walk through some standards and whether judges are involved.

So, I wanted to talk about the difference between their contents of, let's say, a document versus metadata. So, if the Department of Justice wants to get the contents of an electronic letter that is on your home computer, they would need a warrant signed by a judge. Is that right?

Mr. TURLEY. That's correct.

Mr. LIEU. If they want the contents of that same electronic letter stored on a cloud, they will still need a warrant signed by a judge. Is that right?

Mr. TURLEY. Right. If they get at the contents, if they can get metadata, they can show a—

Mr. LIEU. No. I got it. No, no. Let's not confuse things. If they want the same, the content of that electronic letter on a cloud, they will need a warrant signed by a judge, right?

Mr. TURLEY. Yes.

Mr. LIEU. Okay.

Now, let's talk about metadata. First, what is metadata?

Mr. TURLEY. Well, it was defined by one person as basically data about data. That is metadata describes data. That can also then give you information as to the senders, the identification, the subject. That's a lot of information that—

Mr. LIEU. Understood. Okay. So, let's say the Department of Justice wants to get metadata that they believe is stored on your home computer. They would need a warrant signed by a judge, right?

Mr. TURLEY. To get access to a computer, that's correct.

Mr. LIEU. Okay.

Now, if they want to get metadata stored on the cloud, they could simply send a subpoena and get that data without a warrant. Is that right?

Mr. TURLEY. Yeah. In addition, they make companies like Mr. Burt's company essentially the unwilling participants in that type of disclosure. They are being potentially commandeered.

Mr. LIEU. Thank you.

Basic question here. Grand jury subpoenas, a grand jury subpoena for metadata, is a judge involved in that process at all?

Mr. TURLEY. For a grand jury, grand juries can issue for document production at a standard lower than probable cause. Judges are supervising that procedure. In most cases these things are issued with very little review. More importantly, grand jury subpoenas can come under the probable cause standard for document production.

Mr. LIEU. Got it.

So, let's go back to this example where if you had metadata that happens to be stored on the cloud, there is no longer a warrant requirement. What if Congress simply put in a warrant requirement for metadata stored on the cloud, what's your sense of that proposal?

Mr. TURLEY. Well, you could do that, because remember, the probable cause standard is not some huge standard. It's actually—as a criminal defense attorney, I can tell you it's a pretty easy

standard for the prosecution to meet. You have to have clearly articulable facts for getting that type of information.

I don't think that the world come to a sudden stop in terms of prosecutions. It would make this—you would change the grade a bit to make it a little more of a climb for prosecutors.

Because right now, this is similar to the false lantern approach in the East Coast when people would put a lantern to confuse people to think there was safe harbor and this was a lighthouse.

So, people go to the cloud thinking—correctly—that the cloud has lots of protection for their data, and it turns out it's a myth once you do that.

Mr. LIEU. Thank you.

Now, I am sensitive to the view that we don't want to draw lines around certain groups of people and not others. I do know that the Constitution specifically talks about the free press. So, journalists are in fact in a different category.

The Constitution also does put in just structurally separation of powers. When you have one branch, the Executive Branch, trying to intimidate, for example, Congress and seizing all sorts of information, that does pose problems.

So, my view is that we could, in fact, try to do something different. I want to get your thoughts. What if the Department of Justice, when they are getting information on either journalists or Members of Congress, they had to provide notification, for example, to the Department of Justice Inspector General, just as sort of a second check on exactly what they are doing? What do you think about that?

Mr. TURLEY. I think that would be a great idea in terms of greater transparency.

I want to note that some aspects of this confuse me. You have three former and current Attorneys General saying they were not aware of this program. That's not supposed to happen. Since the 1970s, either the Attorney General or a Designated High Official is supposed to sign off on this.

So, I don't know what happened there. It's one of the first things I think this Committee should try to find out about.

Mr. LIEU. Thank you.

My last question is to Mr. Burt at Microsoft.

This increase in these secrecy orders, do you know what the investigations are about? Could it be, for example, about child pornography or something else? Does the DOJ tell what those investigations are about?

With that, I yield back.

Mr. BURT. We don't always know what the investigations are about. We do know enough to know that in the vast majority of these cases they are just routine investigations that are not about child abuse online or about national security issues, but they're just routine.

I do want to make one thing clear, because I may have contributed to this confusion. When we talk about a standard like the warrant standard, the probable cause standard for a warrant, yes, we have to get a warrant before we produce content, email for example. Just a subpoena is all that's necessary to get metadata from us.

What we are here talking about today is the secrecy order that accompanies that warrant or that subpoena. It's there that we need a higher standard and actual findings of fact to establish that a secrecy order is truly necessary.

Mr. LIEU. Thank you.

Chair NADLER. The gentleman yields back.

Mr. Fitzgerald.

Mr. FITZGERALD. Thank you, Mr. Chair.

Sometimes I think we are kind of our worst enemies on this, whether it's Congress or as the judiciary was brought up earlier.

Could you comment, Mr. Burt and Professor Turley, a little bit about changes or accommodations that have been made under the auspices of either national security or public health when it comes to kind of watering down of how this is viewed?

Mr. TURLEY. Do you want to start?

Mr. BURT. Go ahead.

Mr. TURLEY. Well, there's been a lot of changes. The interesting thing is this body has shown that it can solve problems. You did that with healthcare information. You created added privacy protections. You've done that in creating new limitations on secret searches. All that can be done if you have the will do it.

What we're really talking about here is not interfering with investigations, but to require a greater level of transparency and proof, but also to allow greater numbers of people to have access so they can raise it.

This is a problem that we have a lot in national security litigation that I do, and that is the government often wants to do ex parte, in camera presentations and I'm in court screaming bloody murder, saying diplomatically to the judge, "Judge, I know you are familiar with this, but you're not familiar with this case. You need somebody who knows what this case is about to spot whether these documents are material." So, that's a longstanding problem we have.

The problems we face in classified trials are nothing like what is being done here. Basically, people are told they have no ability to challenge it.

Take a look at the Gonzales case out of the Second Circuit. In that case, *The New York Times* reasonably said, "No, we're not going to turn over our phone records to you," and then called their provider and said, "By the way, if they ask for our phone records, please tell us so that we can go to court." The provider said no, no doubt because the Department of Justice said don't tell them.

The Department of Justice's position in Gonzales was *The New York Times* had no standing to be heard on this issue to appeal this question. In what universe of due process would that seem reasonable to you?

Ms. FITZGERALD. Mr. Burt.

Mr. BURT. I would just add that what we've seen happen over the last two, three decades is that tools that were provided to law enforcement to address a particular problem and a particular concern, especially around national security, have now been overtaken by technology and the way that people keep and store their data.

Those tools have now not been restricted and limited in an appropriate way to protect individual rights as technology has moved data from, say, on premises into the cloud.

That's what we're seeking here, is a restriction on those tools that still enable the kinds of investigations that are truly necessary to be conducted for a brief period of time in secret, but that in most cases enable notification to our customers when their data is being obtained.

Mr. FITZGERALD. Thank you. Thank you very much.

Professor Turley, let me get a little more specific and down into some of the issues that had been discussed earlier by some of my colleagues.

The 2017 report by Chair Ron Johnson on the Senate Committee on Homeland Security and Governmental Affairs found that the Trump Administration was facing about 125 leaked stories, about one a day. The report concluded that the leaks, with the capacity to damage national security, which is what I was trying to tee up earlier, flowed faster under President Trump than during President Obama and even George W. Bush.

Why is this problematic? Why was there a difference between Administrations? Ultimately this misleading narrative that's been out there needs to be addressed. I'm just wondering what comments you might have on that.

Mr. TURLEY. Well, frankly, I've never seen leaks like the ones we saw in the Trump Administration. They were occurring so frequently it was almost like you were getting leaks in real time. You would get leaks about meetings that just happened.

That obviously can't happen. You can't have a functioning Presidency if you think that whatever you told the world leader, or your aides is immediately going to be heard on CNN or FOX. The government has legitimate reason to hunt leakers.

My objection is what I call reverse engineering. Nobody can contest that the Trump Administration, when it announced it was going to go after leakers, had every right do that, to go try to find out who was leaking unauthorized information.

What concerns me is that it's always tempting for prosecutors to reverse engineer. They know who received information. Just look at the byline on the article, that's the person who is the recipient.

So, you can reverse engineer by just focusing the investigation on the reporter and then working back to the sender. That's a very dangerous approach. It's dangerous for the Constitution.

The preferred system is to look at the suspects. In the process of that, you're going to find out the numbers of reporters, you have to, otherwise you're going to stop all leak investigations. It's where you start. My suspicion is this might be a case of reverse engineering which I'd love this Committee to confirm.

Chair NADLER. The gentleman's time has expired.

Mr. Raskin.

Mr. RASKIN. Thank you, Mr. Chair. Thanks for calling this hearing in the immediate wake of revelations that the DOJ sought the telephone and email records not just of journalists, but also of two of our colleagues, Mr. Swalwell and Mr. Schiff, as well as even family and staff members apparently.

I want to thank the Witnesses for helping us examine the threats specifically posed to the freedom of the press by these practices. I think it's a matter of fundamental importance to American democracy.

I'm pleased to note that tomorrow I will be introducing the PRESS Act, the Protect Reporters from Exploitative State Spying Act, which I've been working on with Senator Wyden for some time, along with my colleague Mr. Lieu.

This bill is an update of the Free Flow of Information Act that I proudly introduced in the last Congress with our colleague, the Ranking Member, Mr. Jordan, in the 115th.

It will prevent Federal law enforcement from being able to obtain information from covered journalists through their work devices and accounts, as well as their personal devices and accounts.

It will also prevent the government from conducting an end run around these prohibitions by preventing them from seeking third-party communications held by computing and communication services except in narrow exceptional circumstances.

I hope that colleagues on both sides of the aisle, as demonstrated by what appears to be broad consensus today, will join us in co-sponsoring this bill and work to defend the freedom of the press against these practices.

Ms. Burton and Ms. Oberlander, I'd appreciate if you could expound on the need to address the secrecy orders being used by law enforcement to prevent targets from even being aware that their information is being sought and what type of oversight the court should be conducting to rein in the abuse of secrecy orders.

Ms. BURTON. Thank you, Congressman.

I would suggest that by having again a narrow procedural bill which does that, there cannot be a secrecy order without a compelling interest that's been identified and presented to a judge very specifically and a judge has actually made a ruling. That if we did that, you would see very few secrecy orders, because before we had this back door that everyone was going through, it wasn't a problem at the same levels that it is now.

So, I would just suggest that if we have proper and clear requirements that there is a bilateral presentation to a court, either through the judiciary, which would create some opportunity to hear the other side of an argument if something really was a national security issue, a very narrow set of cases, that would probably resolve the secrecy issue.

Mr. RASKIN. Then the secrecy order would go back to being an exceptional case, rather than the rule now.

Ms. BURTON. Exactly.

Mr. RASKIN. It seems to be pretty perfunctory that they get them now, right? Yeah.

Ms. BURTON. That's right. It's having a dual process and it's having a presumption in favor of openness that judges respond very well to, in light of all the constitutional rules and cases that have upheld those basic tenets.

Mr. RASKIN. Okay.

Did any of the other Witnesses want to comment on that?

Ms. OBERLANDER. I would only add that there are a couple other things we can do, too.

So, as we've discussed, narrow the length of time that these secrecy orders are in effect by putting a cap on them in the statute. Right now, in 2705(b), there's no time limit. So, you add 45 days or 90 days, and that's it, you then have to tell the subject, the media entity, that their materials have been requested, that would help as well.

Then the other thing that has been presented in some of our testimony is that, in cases where it's truly necessary to not inform the affected media, maybe we can have an independent third party, some sort of advocate, perhaps who doesn't necessarily let the media know that they've been hired, but who comes in and talks to the judge and says, these are the First Amendment—these are the very, very important First Amendment interests here and you should please be considering them. So, adding, sort of, another to the process.

Mr. RASKIN. Then, Ms. Oberlander let me just stick with you for a second. You noted in your testimony some of the policies that are being used by DOJ to limit the use of subpoenas against journalists, but you observed that these are merely internal policies that are subject to override at whim by future Administrations and they don't address the end runs that are being conducted routinely by law enforcement to obtain third-party data from companies like Microsoft, as noted by Mr. Burt.

I wonder, what do you think about the need for a fresh shield law, given everything that we've learned in last few months?

Maybe I can close just with that question to all the Witnesses.

Ms. OBERLANDER. I am delighted to hear that you're introducing the PRESS Act tomorrow. We absolutely need a shield law, which will, frankly, protect from government overreach but also in private cases, as well, and civil cases. So, I really think we absolutely need it, and I'm really thrilled to see that Congress is working towards—

Mr. RASKIN. Next, just if I could go down the line there, Professor Turley, do you agree we need one?

Mr. TURLEY. Oh, I do agree. The only quibble I had in my testimony is on the—it's more than a quibble, is a disagreement about the definition of covered persons.

I also think that it can be tweaked to increase some issues. For example, there's a single line, "National security may be considered by a court," that's in the previous legislation, and it really doesn't say how that should be weighed by the court. I expect a lot of judges would look askance at that as a standard.

Mr. RASKIN. Okay.

Ms. Burton, do you agree?

Ms. BURTON. I agree, but I wouldn't let that process, which will be a longer process, stop this Committee from issuing a bill and a law right away. I think that we cannot underestimate the harm of privacy and the harm of a lack of process here, which, to me, is incredibly dangerous to the American public. I do support a shield bill. I think it's a more complex discussion which we should be reflecting on also.

Mr. RASKIN. Thank you.

I yield back, Mr. Chair. Thank you for your indulgence.

Chair NADLER. The gentleman yields back.

Mr. Jordan.

Mr. JORDAN. Thank you, Mr. Chair.

I want to thank the Chair for putting this hearing together today on this important subject. I was just thinking about, in kind of a broad sense, how serious this situation is.

Americans have a Fourth Amendment expectation of privacy regarding all their information, including, as we've talked about, information stored in the cloud. Yet, government can come to a third party, like Mr. Burt's company, and, with something less than a warrant, get that information. When government does that, they tell Mr. Burt that he can't tell his customer what's going on, he can't tell his customer that, hey, your Fourth Amendment liberties have just been violated. When government initiates it all, the Attorney General doesn't even sign off on it.

Now, if that's not serious—the current situation that brought us here is the situation that has been in the press. We have had Mr. Barr, I think it's in Mr. Turley's testimony. He says, very first point, the authorization, "It's notable." I'd said it's more than notable. I'd say it's shocking, it's alarming, that Jeff Sessions, Bill Barr, and Merrick Garland all deny any knowledge of what took place. Somebody had to sign off on it.

So, you've got the fundamental issue at stake here, and you got no one who's been Senate-confirmed—which is part of our checks and balances on protecting our liberties—who's even signed off on this.

So, I find this—as Mr. Gaetz led off on our side, the idea that we can work together on this, Mr. Chair, and do something, whether it's the shield law that I've cosponsored in the past with Mr. Raskin or what have you. That is the situation.

I'm just curious, Mr. Burt, has it happened to the same customer several times?

Mr. BURT. I'm sure it has happened to the same customer several times, although I can't say that with any specificity. I'm sure it has happened.

Mr. JORDAN. So, it could even be worse than I just described.

Mr. BURT. It could be.

I would just—one thing, Congressman, is that one of the things we always do when we get these processes, we look to make sure that it's adequate. We will not produce our customers' content, our email or other content, without a warrant. We require a warrant.

We still get subject to the secrecy order, so we can't tell the customer that their data's been taken. Only the customer can actually exercise their Fourth Amendment right. You can't exercise your right if you don't know it's been violated.

Mr. JORDAN. Even when you suspect it might be and they tell you, as in the Gonzalez case, which Mr. Turley has cited, they can specifically say, no, you can't even—they can't do it. There's no way to go make your case and be an advocate and do what you need to do in a court.

Mr. BURT. That's right. The court would say, we don't have standing on the Fourth Amendment issue. We would be told we don't have the right to tell our customer that they should go look to see if their Fourth Amendment rights have been violated.

Mr. JORDAN. Okay.

So, Mr. Turley, what should we do? This may be the first time this Committee, this Congress, has actually had some kind of agreement on maybe we can work together on something. So, tell us steps one, two, and three, what you think we should do.

Because the idea that Mr. Raskin and I, who don't agree on a whole lot, agree and we've cosponsored this legislation is telling. You've heard the comments from both sides.

So, give us the one, two, three that the Congress of the United States should pass.

Mr. TURLEY. Well, putting aside the shield law, which we discussed, I note there are six areas I think should look at, but I think that you need to strengthen these standards. You need to give courts more concrete standards, give standing to companies, like Microsoft, like *The New York Times*, to be able to contest these issues, to limit these types of agreements.

You've got to stop relying on the goodwill of Department of Justice. Department of Justice says that these types of orders have to be, quote, "extraordinary measures," not standard investigatory practices. If the reports are true, as to what we've been reading about, then that and a buck will buy you a cup of coffee. It was not worth the paper they wrote it on. You need to establish concrete standards that can be appealed, and that the critical parties of interest can be in that room.

Then we also need greater transparency on how many of these things are being issued and their conditions. You have a number of courts that have complained in writing that they're getting nothing but boilerplate language from the Justice Department and little ability of the court to say no.

Mr. JORDAN. Great.

Thank you all.

Mr. Burt, you wanted to—

Mr. BURT. Yeah. We detail in my written testimony the steps we think the Committee should consider, but I could just emphasize a couple of them as really critical.

First, the restriction on us telling our customer is a restriction on our First Amendment right. A number of courts have recognized that, which means that the standard of a secrecy order should be a strict scrutiny standard. That's not being applied. So, the corrective legislation would be clear that strict scrutiny should be applied and that there must be findings by the court based on compelling evidence submitted to the court showing that standard has been met.

Even then, these privacy orders should never be longer than, we propose, 90 days without clear evidence being shown later on as to why they should be extended.

We think just those steps would significantly reduce the number of these privacy orders that are even sought and would certainly reduce the number that are being granted and confine them to those cases where they are truly necessary in the national interest. Because they would have to show, to get that privacy order, that they can meet one of those five statutory bases for getting a privacy order, which are reasonable reasons to proceed in a short-term, private, secret way.

Chair NADLER. The gentleman's time has expired.

Mr. Jeffries?

Mr. JEFFRIES. I thank the distinguished Chair for holding this hearing, as well as the Witnesses for your presence here today.

Clearly, in the constitutional construct of this country, we've got an Article I Legislative Branch that I'm very proud to serve in, the Article II Executive Branch, the Article III Judiciary, all apparently constructed to make sure that there are checks and balances.

Also, I think the Framers of the Constitution recognized the importance of a free and fair press. It's in the First Amendment, the first decision made to amend the Constitution, recognizing that perhaps a fourth estate was also central to their vision as to what the democratic Republic would look like, were we able to keep it.

So, I just wanted to ask a few questions, and, Ms. Oberlander, I'll start with you. Throughout your career, you've advised media companies and journalists, I believe, on the legal implications of reporting on matters of public concern in national security. Is that right?

Ms. OBERLANDER. Yes, that is.

Mr. JEFFRIES. In your view, how has the government's use of, what I would phrase, secret subpoenas and gag orders threatened the ability of journalists to actually do their job?

Ms. OBERLANDER. So, journalists who are afraid that they are being surveilled or even that they have been surveilled in the past or that they are—it's very difficult to go and convince or talk to or be able to fairly represent to a source that they will try to maintain their confidentiality. It's quite chilling.

I mean, some of it is on the source side, where they hear—they see that the journalists have been subject to subpoenas after the fact, and they say, "I can't talk to you." It makes it very, very challenging.

Mr. JEFFRIES. Is it fair to say that, in providing information to the public, which is a great service, that the media, the fourth estate that journalists provide, that they often will rely on confidential sources? Is that right?

Ms. OBERLANDER. Yes. There's a lot of reporting, national security reporting but also all sorts of other very important reporting, that relies on confidential sources.

Mr. JEFFRIES. Can you elaborate on the importance of maintaining confidential sources without, sort of, this practice being chilled by an overbroad or overly aggressive Department of Justice utilizing these secret subpoenas to try to unroot these sources?

Ms. OBERLANDER. Well, yes. If you—in our papers, in the testimony, you can look at all sorts of incredibly important stories of, really, national importance that were based on confidential sources. Some were, in fact, national security stories, but others were conditions at Walter Reed, levels of corruption in foreign governments.

In fact, frankly, as a person who has worked at Univision, I can report that there's an awful lot of reporting about what's happening internationally with other governments, not the American Government, where you have very, very important reporting coming through and where the sources are literally afraid for their lives.

So, if you cannot maintain their confidentiality, if there's a risk that they're going to be disclosed, then they really are—they may

be killed. They have very legitimate fears of retaliation. That, of course—fortunately, we tend not to have killed too many journalists or sources here that I'm aware of in the U.S., but it's definitely a big part of our reporting.

Similarly, there have been reports, much reporting, about all sorts of fraud: Fraud in H–2A visa applications, things that are relying on confidential sources, people who don't want to be disclosed because they may be here, they may be undocumented, but they still may be subjected to quite horrible conditions; the Enron reporting; the BALCO reporting; and, just now, even the reporting about the tax filings of wealthy Americans.

Mr. JEFFRIES. Now, in justifying what some of us may characterize as overly aggressive and/or inappropriate behavior at times, Department of Justice or other governmental entities will sometimes cite national security. That's a very broad phrase. Certainly, all are concerned about national security.

In your experience, can you just, in the final few moments that I've got, articulate whether that is being invoked in an overly broad fashion? How might we think about viewing and balancing national security as a concern but also allowing the free and fair press, as vital to our democracy, to also be able to thrive?

Ms. OBERLANDER. So—

Chair NADLER. The time of the gentleman has expired. The Witness may answer the question.

Ms. OBERLANDER. So, there's a longstanding problem of overclassification of information in the country. Because of that, if a source discloses some information that is classified and maybe gives the government an opportunity to argue that the disclosure is a violation of one of the secrecy acts or the Espionage Act, you all of a sudden have a national security issue, when, really, much of that information is not of that kind of importance where you would be disclosing something truly secret and dangerous to the country.

So, one way of restricting it is to restrict the definition of "national security" in any of the statutes that we pass—I mean, in terms of what would qualify for an exception—and to narrow it, maybe, as has been proposed, just to include terrorists and potential terrorist acts, a really dramatic issue, and not just a level of embarrassment to the government. That would be one approach.

Mr. JEFFRIES. Thank you.

Chair NADLER. Mr. Bentz?

Mr. BENTZ. Thank you, Mr. Chair.

Thanks all the Witnesses for their excellent testimony and their doubly excellent testimony as it appears in my notebook here.

We had a 25-hour, marathon discussion about Big Tech just last week, and much of that discussion focused on eroding thoughts about privacy.

So, Professor Turley, I think you mentioned that the reasonable expectation of privacy perhaps isn't as reasonable as it once was, given what we're now doing.

So, your awareness of that space leads me to ask you, what is our new standard? What's the alternative if none of us should expect privacy anymore in this dual life we live, one online and one sitting here today?

Mr. TURLEY. Well, I think that is the danger, that we could move towards a post-privacy world. That's something that none of us wants to see happen.

The Katz standard is unlikely to change, but it means that our protection from government surveillance is based on our reasonable expectation of privacy. As that expectation falls, the government's ability to engage in warrantless surveillance increases, and that can make expectations fall further.

This is the ultimate example of that. People store a great deal of their information on the cloud. As they begin to understand that what they send in messages, in terms of metadata, is not protected and phone numbers are not protected and all these other areas are treated as just subject to the standard of reasonable suspicion, which is barely a speed bump for prosecutors, their expectations will decline further.

What worries me is—I tell my students this all the time when I teach privacy at the law school—is that my students' expectation of privacy is a fraction of my own, and we're seeing this decline in generations. It has real impacts on government ability to engage in warrantless surveillance.

That's why this is an occasion where the Congress actually can correct the error of the courts, can come in and say, we actually don't want to live in a post-privacy world. There is new technology here, particularly on the cloud, and we're going to protect it.

Because if we're really serious about Katz, that the Fourth Amendment protects people, not places, then go protect people. You find them in the cloud, in terms of what they are leaving there. Then you would actually defend Katz more than the Supreme Court has done.

Mr. BENTZ. Thank you, Professor.

Let's move to Ms. Burton, then.

On page 11 of your written testimony, you note that there had been a constitutional violation, I think was the way you put it, preventing a lawyer communicating with their clients by virtue of one of these gag orders.

Are you familiar with any other situation where such a prohibition has occurred, where a lawyer has been told by a judge, you can't talk with your client?

Ms. BURTON. No, I'm not aware of one, Congressman. I think it's a clear violation of prior restraint laws and the attorney-client privilege laws. If I had been subject to that, I would've brought a separate action in the courts to have that vacated.

Obviously, that's not something that should—you shouldn't need to do. It should be part of continuing legislation that we're considering today.

Mr. BENTZ. Right.

At the bottom of the paragraph, your last sentence, you state, "Any legislation should clarify the extraordinary presumption against such orders and the heavy burden that government must bear to justify one."

Would you describe how—or tell us how you would craft the definition of that heavy burden.

Ms. BURTON. Yeah, I think there has to be a compelling interest before any kind of a secrecy order can be imposed.

One of the things we've done is we have contractual provisions with all our cloud providers that require them to give us notice. So, that has actually helped, which tells me that if we were to add some language into statutes, we would have the same benefit of that.

The government will typically go to whoever is easiest to get the information from. If there's a battle over a contractual provision, I give credit to Microsoft, they've been very good at giving us notice, but that's not the case in all our communication providers.

Mr. BENTZ. Well, thank you.

Thank all of you for your patience.

I yield back.

Chair NADLER. The gentleman yields back.

Mr. Swalwell?

Mr. SWALWELL. Thank you, Chair, and thank you for holding this hearing.

As we look at the last Administration and the abuses at the Department of Justice, it's clear that we had a President and a Department that rewarded the President's friends, reducing the sentences or issuing pardons for Paul Manafort, Roger Stone, Michael Flynn, and then punished and weaponized the Department to go after the President's enemies.

I guess I'll start with Ms. Oberlander, if you would engage me on this. Would you agree that Presidents set the tone for a country, that how a President engages, whether they're a bully or they're compassionate or they're a leader, has a real effect on just how everyday Americans can carry themselves?

Ms. OBERLANDER. I would. I do think that the attacks on the media of the last Administration have had a profound and negative effect on how the media is perceived by all Americans. I think the cries of, "fake news" and the specific attacks on particular journalists has really undermined and worked to really injure the standing of the press.

Mr. SWALWELL. Ms. Oberlander, you're correct. We've seen at the Trump rallies the attacks on the media. We've seen, across the country, attacks and violence against journalists. You did not know my questions ahead of time.

Mr. Chair, this is not an advertisement for my violence-against-journalism bill.

Ms. Oberlander, my concern, aside from what Donald Trump and the Department did—because I have faith that Merrick Garland is going to get to the bottom of this and that in Congress, we will understand exactly who was responsible.

To kind of extrapolate what you were saying, the Department of Justice is not the only law enforcement agency in America. Is that right?

Ms. OBERLANDER. I think that's correct, yes.

Mr. SWALWELL. In every State, you have a State Attorney General and, of course, county and municipal law enforcement.

Ms. OBERLANDER. Yes, you do.

Mr. SWALWELL. Do you fear that if you have a President who was willing—who detests accountability and was willing to weaponize his own law enforcement agency against his enemies, that could have the effect, just as we mentioned earlier with the President

setting the tone, of governors and mayors seeing it as a permission slip to weaponize local law enforcement?

Ms. OBERLANDER. Well, I do want to say that the subpoenas to the media have been going on across—this is not a partisan issue. I mean, we did see that President Obama issued a number of—there were more leak investigations than there had ever been, and that's continuing—we've had a growth of that.

So, it's not purely a political issue, but, yes, the attacks on the media have had an effect both Federally and at local and State jurisdictions.

If you look at the—there's been a lot of video of how media, who were labeled "Media," "Press," et cetera, were treated and injured during some of the protests last summer. It does feel that, in some cases, they were singled out because they were press.

Mr. SWALWELL. To distinguish—because I agree with you; it was wrong that the Obama Administration allowed that. Would you agree that, while that was an aggressive pursuit of leaks, the difference between what we have seen or suspect with the Trump Administration is that it was a punitive use of power, meaning it was used—the motivation was to go after perceived enemies, whereas on the Obama Administration side it seemed it was an aggressive use of law enforcement? Wrong, but I think there is a distinction.

Ms. OBERLANDER. I mean, there is absolutely a distinction between the way the Administrations operated. I wouldn't want to characterize one motive or the other on that front.

I will say that there has been—during the Trump Administration, we believe that there have been twice as many leak investigations opened up as there were in the prior Administration.

Mr. SWALWELL. Ms. Oberlander, I don't want anyone to walk away from this hearing believing that Members of Congress think that they are above the law. If a Member of Congress commits a crime or if there's probable cause for a search warrant, he or she should have their records subpoenaed or their property searched and seized.

What can we do—aside from additional protections for journalists, what can we do for non-journalists, as far as additional protections?

Ms. OBERLANDER. So—and I completely agree. I will say that even the shield laws that we've looked at and all the Attorney General guidelines—I do want to point out that, if a journalist is suspected of committing a crime not related to news gathering, that the crime is not itself growing out of the news gathering, then none of these protections apply. The government can come after and look for their materials and see if—so there has always been an exception, a carve-out, for crimes that have nothing to do with news gathering in all of that.

I do think that—for everyone, I do think there should be, at the very, very least—and this applies to Members of Congress—a duty of candor on the part of the Department that, any time they are looking for materials from a Congressperson or their staffs or their family and they know whose materials they're looking for, they need to tell the third-party provider or the service provider of whose information it is.

Apple has said that they had no way to identify—essentially, that they didn't know that this was congressional staff and families. So, I think there should be a legislative obligation to disclose what they know and why they're looking for it. Then in the limited, very limited, places where there is no notice given, the service provider will be able to make a determination of whether that's something that they should be objecting to or not.

Mr. SWALWELL. Great.

I yield back.

Chair NADLER. The gentleman's time has expired.

Mr. Johnson?

Mr. JOHNSON of Louisiana. Thank you, Mr. Chair.

I appreciate our Witnesses, but I have to use a few moments here to address the elephant in the room. I am here at the southern border, La Joya, Texas, participating remotely, because we're here with President Trump, with Governor Abbott, and about two dozen Members of Congress to highlight the crisis here.

Mr. Chair, I have to say, our Committee, the House Judiciary Committee, has jurisdiction, broad jurisdiction, and this is the most pressing issue facing the country, and it's being totally ignored by the Committee. We have to point that out.

Last night, Mr. Chair, we were on the border until probably 1:00 or 1:30 in the morning. We watched just droves of migrants in caravans coming across the border all night, completely undeterred, because the border wall construction was stopped there just south of La Joya. There's a big, gaping hole. There are many, of course, all across the southeast Texas border.

We appreciate Vice President Harris finally making a trip to El Paso, but that is not where the crisis is at its apex. It's here in south Texas, many hundreds of miles south of where the Vice President went.

The House Judiciary Committee has a responsibility to address this crisis. We had 180,000-plus encounters at the southern border just in May alone. It is a record increase, and it is a crisis.

We saw small children abandoned last night at the border, walking across unaccompanied. The Border Patrol—Customs and the Border Patrol—Protection—the agents here are so frustrated because they can't stop it. All they can do is work as processing agents for the cartels who are trafficking humans into this country. They take them to a facility. Most of them are not COVID-tested. They give them travel arrangements, and they're sent into the country to all points, all 50 States apparently, with no expectation that they'll be tracked or returned at all. This is a humanitarian crisis.

Oh, by the way, fentanyl seizures are up 934 pounds at the southern border alone just in May, a 300-percent increase over May of last year. This affects every State in the nation and every American, ultimately. It is an outrage. It is a dereliction of our duty.

I'm saying to my colleagues on both sides of the aisle, we must address this. The Republicans on our Committee have introduced legislation to fix this. I've got a number of bills myself to help with the asylum reforms and all the things that we know need to be done. But they have been ignored.

I just want to go on record and use my time this morning to say, we will be highlighting this today on the border. We hope that the media covers this and shows the American people what's going on. I think, very frankly, and I say respectfully, Mr. Chair, it is a shame the Judiciary Committee is not doing anything about it.

I will yield back my time, because I'm about to go to the border here. We need to talk about this, and we need to have a hearing. I yield back.

Chair NADLER. The gentleman yields back.

Ms. Jayapal?

Ms. JAYAPAL. Thank you, Mr. Chair.

I hope Mr. Johnson will ask Donald Trump why he separated thousands of children from their families. I hope he asks him why the Department of Justice under the Trump Administration undermined the civil liberties of so many people across the country with these secrecy orders.

I wanted to pick up on, I believe it was, Mr. Cicilline's questions about what is needed to get these protection orders. I think that this whole process is really quite stunning for most Americans, who don't distinguish between what happens to their data that's stored and what would happen if they were to be in their home and their files were to be seized.

So, I want to just read from—this is a U.S. Department of Justice Office of the Deputy Attorney General memo from October 19th, 2017. In the footnote, it says, when applying for a 2705(b) order to accompany a subpoena that is—to accompany a subpoena seeking basic subscriber information in an ongoing investigation that is not public or known to the subject of the investigation, "stating the reasons for protection from disclosure under 2705(b) usually will suffice."

It actually just puts a point on—I think every one of you, in some way or another, has commented on this. I think, Mr. Turley, you were speaking to this as well. It's quite stunning to me that there really seems to be no standard at all. So, of course, the courts are not going to get any information, because the direction is you don't need to provide it.

So, I'm wondering, on a scale of 1–10, of one being a rubber stamp and 10 being a real process that protects our civil liberties, our rights, just curious where you would put the current standard. We can just go through quickly.

Mr. Turley?

Mr. TURLEY. I put it at a one.

I really compliment you for highlighting that footnote, because it is how it reads. It's basically telling prosecutors, "Confine what you say. You don't have to give any details."

The Department of Justice benefits from that, right? If you can use boilerplate and use it over and over again, then judges, when they see it, basically say, "This is all they have to show." That's how you get to these high numbers, in terms of the use of these devices.

Ms. JAYAPAL. Mr. Burt?

Mr. BURT. I would agree that it's a one.

While there's that footnote, that same policy, which is the one that emanated from our litigation against the Department, says

that they're supposed to articulate facts. Then when you look at the template that the Department of Justice provides to the 93 offices around the country that says, here's how to get these secrecy orders, it says, "Just write down this boilerplate."

So, the actual form template is consistent with the footnote, and there's really no meaningful process.

Ms. JAYAPAL. Ms. Oberlander?

Ms. OBERLANDER. I mean, I don't have a lot of exposure to these, only the ones that have been reported. Certainly, for the ones that have been reported, one or two, which is pretty low.

Ms. JAYAPAL. Yeah.

Ms. Burton?

Ms. BURTON. I'd put it at a zero. I mean, this falls under the category of a ham sandwich can be indicted.

Ms. JAYAPAL. Right.

Ms. BURTON. This falls into the government calls the shots and that's the end of the discussion. That goes to a zero to me.

Mr. TURLEY. I object. I wasn't given that option when I took the test.

Ms. JAYAPAL. You stuck to the instructions.

Now, let's say, Ms. Burton—and I'll just stick with you on this one—let's say that the extension is obtained and then the very next day the case is dropped because there's not enough—there's not enough evidence, whatever.

What happens to the extension? Does the DOJ go back and say, "Oh, actually, we don't need that extension anymore"? Can you give us some knowledge about that?

Ms. BURTON. Yeah, we have a case where 15 years ago, very, very beginning of cloud computing, it is still a sealed proceeding. I mentioned it in my testimony. So, I think this is a critical problem. You've got to have a sunset provision at the very least.

Again, if you have Pentagon Paper-type standards before you can even enter into this kind of a secrecy order, you aren't going to have a big problem. I mean, national security and secrecy orders are a very small percentage of what we're talking about.

Ms. JAYAPAL. Right.

Ms. BURTON. So, I think you would have a sunset and a small problem.

Ms. JAYAPAL. So, Mr. Burt, I was struck by the data of Microsoft receiving 5,500 requests just in the first half of 2020 and your company turning over basic data to 54 percent of the requests. Compare that to *The New York Times* reporting that Apple turned over basic data in 43 percent, Google turned it over in 83 percent, Facebook turned it over in between 85–89 percent.

It seems to me that we are essentially depending on tech companies, in this case, to negotiate the civil rights and civil liberties of their users. Why is it that your rates—and if Apple were here, I would ask them as well—were so much lower? It seems to me you take this very seriously in how you move forward with these requests.

Chair NADLER. The time of the gentlelady has expired. The Witness may answer the question.

Mr. BURT. Yes, well, we do take it very seriously, because we think it is our obligation to protect our customer interests here and

because we do believe this is a First Amendment violation, a restriction on our ability to inform our customers when the data they trust us to hold securely for them has been taken by the government.

Somewhat in defense of some of my competitive companies, you also have to understand that different companies have different categories of data. So, we have a lot of what has been referred to as "metadata." Often what we get is a subpoena for that metadata then accompanied with a privacy or a gag order. So, our percentage about how often we provide content versus metadata is, in part, a reflection of the volume of accounts where we do have metadata, whereas with a social media company, for example, that metadata might be less interesting to the government. They might be more interested in the content of the postings.

I don't know, because I don't represent them, and I don't see the demands that they get. There are possible explanations other than just how seriously we do take our obligation.

Ms. JAYAPAL. Well, thank you for taking it seriously.

I yield back, Mr. Chair.

Chair NADLER. The gentlelady yields back.

Ms. Scanlon?

Ms. SCANLON. Thank you, Mr. Chair.

Thank you to all our Witnesses for speaking today about these really important issues surrounding the DOJ's extraordinary use of its investigative powers to seize materials from members of the press, Members of Congress, and their staff and families.

As a lawyer and someone who's proud to represent Philadelphia, I had to note Ms. Oberlander's written testimony where she talked about the fundamental values underpinning the First Amendment and the uniquely American principle of valuing a free press.

The first strong expression of that principle arose during the John Peter Zenger trial, which occurred before the Constitution was even written. That case stemmed from Zenger's refusal to disclose the sources of articles critical of the British Government that he published in his newspaper.

Of course, it was the brilliant Philadelphia lawyer Andrew Hamilton—no relation to Alexander—who represented Zenger in that case. Hamilton argued for the critical importance of a free press to preserve our liberty by exposing and opposing tyrannical power by speaking and writing truth. Those principles were written into the Constitution.

How striking that almost 300 years later we're still addressing the same issue. We need to preserve the ability of a free press to protect its sources, particularly from a vengeful or tyrannical government that's trying to prevent the press from speaking and writing truth.

Now, Mr. Burt mentioned the problem that, when data is obtained under a gag order from Microsoft or other platforms, they can't raise the Fourth Amendment protections because those belong to the individuals whose data is being seized, but then we have this catch–22 because they also can't tell those individuals that their data's been seized and thereby give them the right to assert their Fourth Amendment rights.

As I understand it, the workaround here that some news agencies have been able to implement is that they have contractual provisions that require the tech platforms to notify them if the government seizes the data. Then the gag order extends to the attorneys as well, so we still have those problems.

Do I have that wrong?

Mr. Burt, you are shaking your head.

Mr. BURT. Yes. That's not quite right—

Ms. SCANLON. Okay.

Mr. BURT. —because the media companies—we do disclose when we can. We have customers, including some media companies, that have very specific disclosure obligations written in by contract. Because, as I pointed out earlier, we don't have an obligation to tell our customers when their data has been subpoenaed or obtained by a warrant, but we do it as a matter of policy. So, some of customers say, "Well, we want that in the contract," and we agree to that, but it's always subject to the secrecy order.

So, we can't inform the media companies' outside counsel, we can't inform anyone. Even within the company itself, within Microsoft, we're restricted as to who can know about some of these secrecy orders.

So, it's not a workaround for this problem. For the press to exercise its right to be a free press, they have to know when their data is being taken by government. We can't tell them, when we have a secrecy order.

Ms. SCANLON. Okay.

Ms. Oberlander, you discussed the fact that the construct that is being used now creates issues with respect to attorney-client privilege. Is that right?

Ms. OBERLANDER. Yes. I mean, certainly, as when you just extend the secrecy order to the in-house counsel and you don't let them tell their client, yeah. To their outside counsel, for that matter.

Ms. SCANLON. So, does that impede the free press's ability to collect data, et cetera? Who does that impact?

Ms. OBERLANDER. So, first, the attorney can't do what they're hired to do, which is to give advice to their client. In some ways, it's better than nothing, because they can, in fact, hire, if they're permitted to, outside counsel, who can go and try to make their position known to the government, which is what happened with these gag orders that we've been talking about. It's very, very limited.

It also creates—just in terms of the client relationship, if your client doesn't think that you're telling them the truth or that you know something about their work, then there is a level of distrust there that can poison the entire relationship going forward.

Ms. SCANLON. So, it sounds like these processes create a corrosive impact upon the whole system.

Ms. OBERLANDER. I believe it does, yes.

Ms. SCANLON. Mr. Turley, you mentioned that the current DOJ procedures requires senior DOJ leadership to sign off on these secret subpoenas. Is that correct?

Mr. TURLEY. Yes, that's correct.

Ms. SCANLON. As you noted, the three most senior officials at the Department of Justice during the relevant time period, both former Attorneys General Sessions and Barr and Deputy AG Rosenstein, all deny that they signed off on the subpoenas in this arena. Is that right?

Mr. TURLEY. That's my understanding, yes.

Ms. SCANLON. So, do you think the process failed, or are these answers from those officials disingenuous?

Mr. TURLEY. Well, that's the first thing I put in my testimony for this Committee to confirm, because it doesn't make sense to me—that standard of a high level of approval was put in in the 1970s as part of reforms overall. Then, after the controversy during the Obama Administration, it was ramped up again, it was reaffirmed that you need that type of signoff.

This is one of those things that, sort of, should make the sand balance over in the Department of Justice. I mean, if you're coming up with a search that's hitting on journalists or Members of Congress, you would think that would go straight to the AG's desk. I believe these AGs; they don't have any recollection of approving this or being informed of it. That's the first thing that I think the Committee needs to determine, because if that's true, something seriously went wrong here.

Ms. SCANLON. Okay. Thank you.

I see my time has expired, and I yield back.

Chair NADLER. The gentlelady yields back.

Ms. Garcia?

Ms. GARCIA. Thank you, Mr. Chair, and thank you for putting together this wonderful group of experts to visit with us on this very important topic.

Like many Americans, I was alarmed to learn that, reportedly, the Trump Administration seized records, seized records from Apple and others, to obtain phone and email records belonging to some of our very own colleagues, their families, and their staffs. I mean, it was outrageous. Then also from news reporters, which, again, is outrageous behavior.

It appears now from some of the testimony we've heard today that, more often than not, gag orders were sought from the providers to make sure that they could not alert anyone. To me, this is a blatant abuse of power.

During the House impeachment investigations and trials of Donald J. Trump, I constantly reminded my colleagues and all Americans that democracy is a gift that each generation gives to the next. We must protect that democracy, and we must do all that we can to stop this kind of behavior.

Former President Trump has time and time again placed his own personal interests above the American people, and it appears that he did that in this case, too. My colleague Mr. Swalwell, who looks like he was a target of these attacks, mentioned that earlier. It is again looking at and wanting to get some of his critics.

It's evident that our Founding Fathers vested the power in Congress for oversight, so I am so glad they we're doing that today. Congress and the American people deserve the right to know whether these unauthorized disclosures of classified information were properly predicated and approved.

I've said it before, and I'll say it again: Nadie esta por encima de la ley. No one is above the law.

I'd like to start my questions with Ms. Burton.

Ms. Burton, you mentioned in the three or four things that you would seek in reforms, which were—it's just very refreshing that it appears to be true; we seem to have a consensus even in our Committee that reforms are needed, and it looks like we have almost unanimity among the panelists. So, it is a rare day for us in Judiciary.

You talked about safeguards; you talked about transparency. If you could wave the magic wand, what would due process look like to you to safeguard the First Amendment rights and Fourth Amendment rights?

Ms. BURTON. Right. I would make them broader than the First Amendment. I'd make them a constitutional right, where you would give the court the obligation to look at what the government presented, and it had to be very specific, and there had to be a compelling reason before anything could be done in secret. The minute that showing was not made, a series of other protections come in, whereby counsel for the press can come in, there's no secrecy order, there's notice, there's no judges.

I think that it's very important that we have clear, articulated standards of what due process means in this case. So, for example, I think cloud information should be treated the same as file-cabinet information. There's no reason—

Ms. GARCIA. I agree, those have to be separate.

Ms. BURTON. I would put that into the legislation.

So, I think it's a series of waterfall things that would follow, one from another, that would make it a very compelling—and problematic for the government on about 95 percent of the cases that they're now proceeding in secret with.

Ms. GARCIA. Well, thank you.

Mr. Burt, you talked about judicial review, and you also talked about limiting the gag orders to 90 days and an extension requiring a high standard for any kind of extension.

What exactly do you have in mind? Do you feel like the scrutiny for the extension needs to be the same or even higher than the original gag-order application?

Mr. BURT. Well, I think it's the same standard that needs to be applied. It's really a strict scrutiny standard, because you're trying to confine the First Amendment rights of the cloud provider to inform their customer about what's happening. So, you can say, we've set aside that for a 90-day period because we have one of these very rare special circumstances where that kind of secrecy is required in the national interest.

If a court is convinced of that and then puts the gag order in place for 90 days, that should be as long it goes, unless government can come back and establish to the same degree, with the same degree of strict scrutiny analysis. So, you have to come forward with compelling evidence, and you have to show that there is no other alternative that can satisfy the government's legitimate interest. So, you'd have to reestablish that that is necessary for an extension of that 90 days.

There should definitely not be any lower standard just because you got a 90-day gag order. If anything, as you're suggesting, perhaps at least the court should be considering, really, why do we need another 90 days?

Ms. GARCIA. Thank you.

Chair NADLER. The gentlelady's time has expired.

Ms. Dean?

Ms. DEAN. Thank you, Mr. Chair.

I thank all our talented Witnesses for your expertise and advice to us.

Ms. Oberlander, I'd like to compare and contrast some of the things we talked about earlier which has to do with State standards as contrasted with Federal standards. Obviously, we know where we stand on the Federal standards.

I come from Pennsylvania, like my friend and colleague Representative Scanlon. Our shield law is among the nation's strongest. In fact, our State courts have read our State legislation to protect as an absolute privilege any information which could expose the source's identity.

Do you believe our State law or other State shield laws that are much more effective could be used as a template for us here as we craft Federal policy?

Ms. OBERLANDER. Well, I do. Pennsylvania does have a good shield law. New York, where I live, has a very, very strong one, also, an absolute privilege for confidential sources and a qualified privilege for nonconfidential material. I absolutely think that those both could be models for a Federal shield law.

I do think that, because you have such a great experiment across all the different States, that one of the places where the State statutes haven't kept up is on the definition of "journalist."

So, it really does depend on which State you are looking at. A lot of them are—some of them, at least, are tied to the fact that you have to get the protections of the statute, you have to work for a newspaper. Magazine and digital radio, they don't necessarily permit without some challenge. Like, if you're an independent journalist now who is running a subscription newsletter or somebody—I work with a lot of journalists who are professional journalists but they're not making any money.

So, the definition of journalist within that is something that you'd have to look at. I wouldn't necessarily say that the State statutes are models on that.

However, in terms of setting aside an absolute privilege for confidential sources and the qualified privilege, they are.

Ms. DEAN. That's helpful.

I'm thinking of my own constituents, journalists in the Fourth Congressional District, and I have many. They feel—and if maybe you could detail the vulnerability. While they enjoy the protection of a State statute, depending upon geography, politics, and other factors, they are left vulnerable.

Can you detail some of that tension?

Ms. OBERLANDER. Yes. I'm going to use the example of New York again, because that's where I practice.

If you are a journalist, you've done a terrific investigative story, maybe it's malfeasance in New York City government—we'll move

it outside of Federal—but there is—or it's a regular—it doesn't have anything to do with government or it's a private malfeasance kind of investigative story, you have sources—if you get a subpoena from the New York State Supreme Court at 60 Centre Street and they want your confidential source information, who's your source, you can go in, you can wave the shield law, and you don't have to provide your source information. It's an absolute privilege.

Across the street, in the Federal courthouse, there is a different standard. It is a qualified privilege, to the degree it exists. You have to go—and there is something. You do have to go, and you show that—or the government or whoever is looking for the information would have to show that it's highly relevant to their lawsuit, that they've tried to get it from other places, they haven't, and that the balance of equities generally weighs in favor of disclosure, but, as a journalist, you may have to disclose your source.

So, when you're talking, when you're reporting it, when you're dealing with your sources, you can't say to them with any real certainty, "I am not going to have to give up your identity." That creates enormous havoc.

Ms. DEAN. Incredibly dangerous. Thank you for that clear description.

Ms. Burton, it's been, I guess, more than 40 years since Congress passed the Privacy Protection Act. Now, we see government can go directly to third-party providers to compel work product, as opposed to going to the journalists who were protected under the act. The PPA is clearly insufficient.

Knowing the actions of DOJ that have been discussed today, how should Congress specifically continue—and I know you've offered some, but—continue to strengthen protections offered by PPA?

Ms. BURTON. Thank you for the question.

Of course, the guidelines first came because the Department of Justice was end-running constitutional rights. Then, when that barrier was not high enough, they went to warrants. Warrants were easy to get stamped in a court. Then you, Congress, passed the PPA.

Now, we come to communication providers. I think that the legislation that's being considered here, the simpleness of it, without a lot of other pieces, but just the simpleness of it to put procedures in place, is what's going to be relevant not just today, but whatever other forums and venues and technology comes in the future. I think it's about process, not about anything else.

So, that's why I would urge us to get this bill passed into law quickly.

Chair NADLER. The gentlelady's time has expired.

Mr. Stanton?

Mr. STANTON. Thank you very much, Mr. Chair.

I want to say thank you to our Witnesses for spending your day with us and assisting this Committee in its important work.

Back in early June, I, like all Americans, was shocked to find out the Department of Justice had secretly tried to attain email records of multiple reporters in newsrooms like *The New York Times*, *The Washington Post*, and CNN. It is frustrating to me—in fact, it's infuriating, to be frank—that Department of Justice, under Presi-

dents of both parties, has led the hunting expeditions into the file cabinets of news reporters.

Journalists and reporters serve a vital function in our democracy, working relentlessly to keep our public informed. Their work is tough, thankless. Yet, day-in and day-out, they do their work. They investigate leads, they find out facts, and they tell the stories that need to be told.

It is freedom of the press that allows the American people to learn of the actions of their government, both good and bad, to learn of actions like the DOJ secretly surveilling reporters and our colleagues here in the halls of Congress. It is freedom of the press that allows the American people to stay informed, stay safe, to form their own opinions, and to be better citizens.

So now, more than ever, we do need to safeguard the protections of the First Amendment, and this Congress must do more to ensure reporters can do their their jobs.

Congress has, in the past, considered a press shield law. One issue when drafting such a law is the question that we discussed a little bit here today of who should qualify as a journalist and what activities deserve added protection.

We can all point to responsible news organizations and journalists who are longstanding institutions of the press, but what about those others who may not fit the traditional mold? What about an online blog or even someone like Darnella Frazier, the courageous young lady that filmed the murder of George Floyd and won a Pulitzer Prize special citation because of her courageous acts?

Where do you draw the line about who would be covered by such a press shield? I'd open it up to any of the Witnesses to answer that question.

I know, Mr. Turley, you put some of that in your prepared testimony.

Mr. TURLEY. Yes, I did. My objection to the current legislation is that it follows a rather dated definition of journalism. It specifies that this has to be part of your livelihood. It also notes that you should have a supervisor or editor that is overseeing your work.

The fact is the media has changed dramatically. Today, many bloggers perform many of the same functions as reporters. Many reporters are looking more like bloggers. They're engaged in the internet and social media to a degree that they didn't. So, you have this sort of merging.

You also have what are sometimes called net-newsers. Today, polls show that people now mix, as sources of their media, internet and traditional sources. In fact, more people get their news from social media today than newspapers.

So, we have to, as we talk about technology changing, we also have to update our view of what a journalism is—a journalist is. This is not an easy task. I'm not pretending that this doesn't have problems. You can't make everyone a journalist, because, if that's the case, then journalism means nothing. You have to have some way of distinguishing between what people do.

What I have argued is, it should be a focus on what their function is, their writing, as opposed to how much they're getting paid for it.

So, Ted Koppel tomorrow could resign from the network and be writing the same columns he did today. Would that mean he's not a journalist? Under this law, he would not be a journalist, because he wouldn't be making any money at it.

Mr. STANTON. Yeah.

Mr. TURLEY. That's obviously something that we don't want to have, an inherent flaw, in a shield law.

Mr. STANTON. I wanted to ask a question—Mr. Burt, you raised in your opening testimony the issue of blanket requests. This, I guess, is a relatively new phenomenon and obviously very frustrating for you and Microsoft. Maybe some of the other Witnesses have experienced it as well.

Can you explain in a little more detail what—talk to us about that blanket request, what it is, and how we might be able to help you in Congress to fix those blanket requests for information.

Mr. BURT. Yeah. So, a blanket request, like the one we received yesterday—and I think there was another one, actually, I was informed, that came in today—is a secrecy gag order that prevents us from notifying customers not just as to a particular subpoena or a particular warrant but to all subpoenas, warrants, and orders issued in the course of a particular case or investigation.

What that really highlights is the lack of adequate standard to get a secrecy order in the first place. Because that standard has to be particular. The government should have to show that, for any specific request for data, that they can meet the standard, the strict scrutiny standard, necessary to impose a gag order.

To say that you can do that for every request, in even the most routine request for information and data, throughout an entire investigation just shows how this process is being abused.

Chair NADLER. The time has—

Mr. STANTON. Thank you so much. I yield back.

Chair NADLER. The gentleman yields back.

Ms. McBath?

Ms. MCBATH. Thank you, Mr. Chair.

Thanks each and every one of you for being here this afternoon. This is a pretty heavy discussion.

As Americans, we, the people, give our government a great deal of power to protect our national security. These include the authority to collect some very sensitive information and to keep it secret. We have laws, including criminal penalties, to make sure that secrets stay secret when lives are definitely on the line.

What I'm describing is how it's all supposed to work. Government actors are given significant power and tools that they're supposed to use to keep us safe. They're given the weighty responsibility of keeping information so secret so nothing gets out that could actually put lives at risk.

Inevitably, there will be times when classified information is leaked to the press. We all know that. In these moments, it can be hard to tell a brave whistleblower from an unpatriotic criminal. It's often only in the writing of history that we actually will be able to say whether or not a leak was in the public interest or a serious threat to our national security.

So, we have a complex set of tools and laws, and, ultimately, courts are tasked with getting this careful balance just right—the

right of pursuing justice, protecting our national security, and also protecting the free press that is foundational to our democracy.

So, the question before us is whether that system is really working right now, or is it in need of repair?

So, one element of this system is the shield laws, State laws that allow reporters and editors and others to protect their sources. At least 40 States and the District of Columbia have some form of shield law on the books, including the State that I represent, which is Georgia.

I'm going to direct these questions to either Ms. Burton or Ms. Oberlander. Both of you, please, feel free to jump in.

Do these State laws vary in their approach to providing reporters protection from compelled disclosure? Also, to the extent that they do vary, has the State-by-State approach adequately protected our journalists that have been engaged in First Amendment activities?

Ms. OBERLANDER. Well, they do vary. As I previously mentioned, some States have a qualified privilege for everything, where you have to go through some sort of balancing test before you can get it. Some States have an absolute privilege for—most places don't have an absolute privilege for everything—but for confidential sources, they might protect that absolutely. There are variations. They do all provide some level—well, most of them provide some level of protection.

The Federal circuits, as well, have different standards. Again, it could completely depend on what circuit you're in as to what is the standard you have to prove.

So, all of them—the fact that there are these varying standards creates great uncertainty on the part of the journalists and of the people who want to provide them information.

To your point about national security, though, and to the degree that there is an investigation into some type of leak or some other type of national security in that search, it would probably be under the Federal—it would probably come out of a Federal court, if not always. Then you would be faced with the question of which circuit you're in. Again, those standards do vary.

Ms. MCBATH. Thank you.

Ms. Burton, did you want to respond?

Ms. BURTON. Yeah. I wanted to respond to your first comment, which I think is very important, regarding the balancing of national security interests, because we haven't really spoken about that.

The Pentagon Papers case—again, 50 years today—makes notice of that, where you had a judge who was told that national security would result in the killing of many troops. He took a very strong look at all the information and then determined that, while he couldn't be sure, that he had to balance against other rights, which in this instance were the press rights.

So, that balancing and courts that really look at these things carefully, whether it is in the shield law or national security, that's kind of the best you can get. There's lots of fact. There is a patchwork of statutes. We have to rely on the judiciary to do their job properly and we have to require of them.

So, I would say, on the State shield laws, we use a Federal privilege on that, and I think that's the way in which we'd begin to

smooth it. Every State is different and it's very much a patchwork at this point.

Ms. MCBATH. Thank you so much.

I'm about out of time, but I want to thank both of you for really giving us good, detailed answers for these questions.

I yield back the balance of my time.

Chair NADLER. The gentlelady yields back.

Ms. Escobar.

Ms. ESCOBAR. Thank you, Mr. Chair.

Many thanks to our panelists for being here today and for helping educate the Committee and the public about what's at stake.

As we continue to read more information, I hope no more information emerges that there were more Members of Congress, more members of the public, more members of the media whose privacy was violated.

As we may possibly hear more of that, I think it's critically important that the public sees that we take action, and that we're responsive to their right to privacy, and that we are a country that honors freedom of speech and that honors, in many ways, the press.

So, Ms. Oberlander, I'm going to have a couple of questions for you.

I have to respond, as the only Member on this Committee from the border, and who represents a border community, I have to respond to one of my colleagues who has chosen not to govern on this important issue today and has instead chosen to participate in the Donald Trump, Greg Abbott circus that is happening in my State, in south Texas.

For the record, and just so that my colleague know, for the record, apprehensions—or encounters rather—of migrants are actually down this year when compared to 2019. May 2021 versus May 2019, numbers of encounters are actually down.

I think what we're going to see on the floor today and tomorrow probably will be an absence of many of our Republican colleagues, who have chosen to abandon their job here in Washington, DC, in an effort to participate in a political stunt.

Back to the topic at hand. Actually, Ms. Oberlander, in some ways this conversation about the border for me speaks to the importance of protecting the Fourth Estate.

During the last four years, during the Trump years, much of what we learned about what was happening in the immigration space, in terms of family separation, in terms of some of the cruelest, most abhorrent anti-immigrant public policy of our generation, we learned through the media.

I served in Congress, was sworn in in 2019, and much of the information that I gained, even as a Member of Congress, came from the media and came from courageous journalists who had cultivated sources who were shocked by what was going on around them and who were willing to shine a bright light on policy that America deserved to know.

From my perspective, I've been vocal about the Biden Administration continuing to empower the government in the same way, although I do want to recognize that the President has made some

really important statements. Our DOJ is in some ways still engaging in the same way.

Because you work with journalists and publications, can you tell the public what we risk if we continue to go down this road, their access to information, what you've seen, and what lies ahead?

Ms. OBERLANDER. Thank you, Congresswoman.

Yes, I think that if there are limitations placed on journalists or that there is a fear that their confidential sources and their work product is going to be accessed inappropriately, outside the rule of law, then you will see a real diminution in the flow of information. You really will. People will not agree to be—they will not come forward as sources of information.

For example, around the border you had sources within the government who were saying, "These are the policies, this is what I'm seeing." You also had sources, you also had the individuals who were affected by these policies, who really had the—ran the risk of retaliation, of being deported. Yet, they were willing to come forward and say, "Listen, I am being placed here. I am not able to make a living wage. My children have been separated." Many of them were afraid of being identified and being deported.

So, what happens then is, if they don't come forward, the entire public loses that information. We all miss the things that we would like to know to make our decisions, to decide who to elect, how to govern. It is a real diminution of the information available to the public.

Ms. ESCOBAR. It absolutely is. That's why we have to take action. I'm glad to see that there's bipartisan support for that. Look forward to working on the recommendations from this panel.

Thank you, Mr. Chair. I yield back.

Chair NADLER. The gentlelady yields back.

Mr. Jones.

I'm sorry, Ms. Ross.

Ms. ROSS. Thank you, Mr. Chair.

Thank you to the Witnesses for your insights and for your patience. I'm second to last, so if you were wondering when you were going to have lunch, it's coming soon.

As a State legislator, I worked to promote transparency and responsible governance in my State of North Carolina. As a civil rights attorney, I've worked on both Fourth Amendment and First Amendment issues, and done a lot of work with the Press Association and to prevent State agencies and law enforcement from conducting unlawful searches. So, this is a very, very interesting topic for me.

Your testimonies highlight the abuse of prosecutorial discretion and do pose important questions about how we can act to fulfill our duty to preserve democracy and a robust free press.

Unchecked prosecutorial power poses concern for all Americans, regardless of their political perspective. It's important that we usher in procedural and normative shifts that will emphasize responsibility with regard to prosecutorial discretion and secrecy orders on the part of law enforcement.

Freedom of the press and government accountability are the bedrocks of our democracy. This Committee has the responsibility to

address and mitigate the potential for prosecutorial abuse and its actual overreach.

My first question is about business, Mr. Burt, and it seems like business has been unduly burdened by doing the government's work.

So, I'd like to ask you what the incentives for service providers like Microsoft are to challenge legal demands issued by law enforcement agencies when they are legally deficient. You are getting a lot of these requests. Why are you resisting it as much as you are?

Mr. BURT. Well, my title actually is Corporate Vice President for Customer Security and Trust. I mention that because a lot of the work that I do with my organization is designed specifically to try to ensure that our customers can trust us with their data and their information and with their transformation to a new digital world.

So, it's very important to Microsoft as a company that our customers know that in these instances where we are subject to gag orders and we can't even tell them that their data is being demanded by government, that we will ensure that we only respond when those requests are truly valid and legal, and that even then we will challenge those, whenever we have a sufficient basis to challenge those requests we will challenge them if we can, and to try to limit the scope of these secrecy orders.

What we've learned is that litigation just isn't a sufficient tool. The volume's too high, the abuse is too great, and we really need legislative reform.

Ms. ROSS. Can you just remind the Committee about the business burden here? How many people hours? How much money does it cost you every year to deal with many of these illegitimate requests?

Mr. BURT. I don't actually have those numbers. We could provide those later to specifically address that.

We have a very large team that responds to lawful access requests. Globally, it's more than 60,000 a year. As we mentioned in our testimony, there are seven to ten of these secrecy gag orders that we get every day and we have to review those for their sufficiency.

We've litigated, eight or nine cases, and each one of those litigations is expensive, and we have made progress through that litigation.

It is a burden to have to manage this all because government isn't doing its job in an appropriate way.

Ms. ROSS. Thank you. I look forward to getting that follow-up information.

This next question is a follow-up on the definition of who the press is, if we pursue the shield laws.

Ms. Oberlander and Ms. Burton, we've heard from Mr. Turley about this, but do you have anything to add? Because I fear that that might be a place where it gets a little thorny for the Committee.

Ms. OBERLANDER. I mean, I agree with Mr. Turley. I believe that you should look not at who somebody works for, but at what activities they are engaged in, and are they regularly producing or writing or photographing or editing or involved with those people in

putting news out of local, national, State, international importance to the public. It could be a small public. It could be a large public. I would look at that.

Then, around the edges, whatever definition you come up with, there will be questions. I think that then there have always been questions. I think that will be something that a court will have to look at the statute and say, "Well, does this person fall under it or do they not?"

So, I would hope that the definition of journalist doesn't tie us up from not getting a shield law.

Chair NADLER. The time of the gentlelady has expired.

Mr. Jones.

Mr. JONES. Well, thank you, Mr. Chair, for convening the full Judiciary Committee today to examine what we can do to prevent abuses like the Trump Administration's secret seizures of data from the accounts of Intelligence Committee Chair Schiff, Representative Swalwell, and numerous journalists.

Let me be clear about something: The Department must act faster to investigate, expose, and end these abuses. It is long past time for this Department of Justice to right the wrongs of the last one.

I worked for the Justice Department early in the Obama Administration, and I understand that the integrity of the Department is important. That is exactly why this Justice Department's reluctance to make a clean break from its predecessors' misdeeds is so misplaced.

The way to restore the Department's integrity is to repudiate the notion that the DOJ was Donald Trump's personal attorney, not to continue to provide him and his policies pro bono defense.

The Trump Administration may not have been the only Administration in our nation's history to engage in these abuses—in fact, that is well established—but it must be the last.

So, I look forward to working with everyone, on a bipartisan basis, for bipartisan legislative solutions to the challenges that we face.

I want to focus in on something that a number of Witnesses mentioned earlier.

From what has been reported over the last few weeks, secrecy orders, in particular, have prevented the counsels of the targeted media companies from sharing information with their clients. Clearly, these orders strain the rules of professional responsibility and attorney-client privilege.

Ms. Oberlander, you touched on this earlier in your exchange with Ms. Scanlon, but I'd like to give you an opportunity to elaborate. Is there anything you'd like to add about this problem?

Ms. OBERLANDER. Well, I mean, I do want to say that letting somebody at the media organization know about the attempt to get their material is better than not letting anybody know about it. So, the answer is not to not tell them.

It really does create a very, very difficult place for the attorneys. I mean, it creates problems with their relationship with their client. Corporately, if it is a corporate issue, it creates issues with when you can't tell the CEO, or the boss, or the chief editor.

It's really—it's just untenable, frankly. It's not a solution to the secrecy orders to tell just one lawyer and gag them from telling anybody else.

It also is, frankly, a prior restraint and really should be looked at, like my colleagues have said, under the strictest scrutiny. If you can't stop *The New York Times* from publishing the Pentagon Papers, you should have the same standard before you limit their lawyer from telling the other journalists about the request.

Mr. JONES. Ms. Burton, what is your perspective on how these secrecy orders directed at the attorneys who represent journalists and media organizations can threaten or compromise the attorney-client relationship?

Ms. BURTON. Thank you for the question.

I think that a statute that you are all getting closer to drafting here would create a separate cause of action to immediately go into a court to vacate that proposed order before the attorney is gagged.

I have to say that I'm not sure I agree with Ms. Oberlander that it's better that someone in the organization knows. It is so corrosive when that occurs.

So, I would statutorily have a separate cause of action that would give the attorney and the business side of that operation the opportunity to challenge it.

Mr. JONES. Thanks so much.

I just want to string together a few basic but vital concepts from the course of this hearing.

Ms. Oberlander, there is no exception to the First Amendment for legal organizations, right?

Ms. OBERLANDER. No.

Mr. JONES. Nothing in the Constitution exempts leak investigations from the Fourth Amendment's protections against unreasonable searches and seizures, correct?

Ms. OBERLANDER. That's what I believe.

Mr. JONES. That's what I learned as well.

Finally, nothing in the Constitution exempts leak investigations from the Fifth Amendment's guarantee of due process, correct?

Ms. OBERLANDER. That's right.

Mr. JONES. So, as far as our constitutional rights are concerned, a leak investigation is like any other. Yet, from what we have heard today, what passes for due process in these matters is anything but.

I just want to ask a series of questions on notice.

Mr. Burt, I just want to review the notice process with you.

When a subpoena is issued for someone's data to a third-party email or cloud provider like Microsoft and a secrecy order is imposed, the person whose data is seized is not notified in way about the subpoena, correct?

Mr. BURT. That's correct.

Mr. JONES. That secrecy order might extend indefinitely, correct?

Mr. BURT. Unfortunately, that's true.

Mr. JONES. How about when a secrecy order with a limited span does expire? Even then, at the expiration date, the law doesn't guarantee any notice to the person whose data the government has seized, correct?

Mr. BURT. That's correct. There's no requirement the government notify. We always do once the secrecy order has expired.

Mr. JONES. Even when there was no conceivable risk at that point that notifying the recipient could interfere with an open investigation or delay a trial?

Mr. BURT. That's right. There is no practice—

Chair NADLER. The gentleman's time has expired. The Witness may answer the question.

Mr. JONES. Thank you, Mr. Chair. I yield back.

Chair NADLER. The gentleman yields back.

Ms. Bush.

Ms. BUSH. St. Louis and I thank you, Chair Nadler, for convening this hearing.

The secrecy surrounding the issuance of the electronic surveillance and accompanying gag orders is deeply concerning and in many ways every actor is implicated—from the Department of Justice, which in this case has abdicated its role to uphold constitutional protections, to the private companies that follow the Department's orders without any transparency, to the legislators who have thrown their hands up and allowed the DOJ to transgress without any accountability and transparency.

While it is shocking to hear that the DOJ was engaging in such surveillance practices against government officials, their staffers, and their families, it is not an anomaly. As a protester and activist, I know firsthand how invasive law enforcement surveillance can be.

It's for this reason that I have been vocal in my opposition to DOJ's blanket ability to surveil all Americans, especially Black and Brown protesters who have been sounding the alarm on this issue.

The Department's ability to surveil Americans exercising their First Amendment right to protest has built the infrastructure that has now allowed the department to surveil Members of this body.

Companies like Apple and others are then left to hand over the records at their disposal, betraying the trust of the people who use their products.

In this instance, Apple complied with the DOJ, demonstrating the thorny position of tech companies balancing their customers' private online activity with legitimate requests from this country's chief law enforcement agency.

Mr. Burt, it has been reported that some data hosts or providers have challenged the government's electronic surveillance orders and the gag orders. However, the companies' ability to challenge the orders is limited and it is not assured.

Mr. Burt, how does the abuse of secrecy orders affect investigations against Black and Brown communities?

Mr. BURT. Well, I think, as you point out, you always have to be aware of the fact that government, as a majority institution, can sometimes disproportionately affect those in minority positions or who have less representation.

Therefore, our Constitution and the constitutional rights on which our country is founded are designed to protect those minority interests and those minority rights especially.

That's why, when you have a law enforcement agency that's able to act secretly, without creating the adequate record to be able to challenge and review those secrecy orders and understand the

basis for them and to ensure that they're only issued when absolutely essential in the national interest, there is almost certainly going to be disproportionate impact of that secrecy.

Ms. BUSH. Thank you.

Can you tell me, how do you decide which orders to challenge?

Mr. BURT. Unfortunately, in most cases we don't know enough, because we are provided so little information, we don't know enough to even know when we have an opportunity to challenge.

We challenge those that on their face are inadequate or clearly not legal, and in most cases, we find prosecutors then agree and withdraw that. That's a big percentage that we challenge. We also challenge those that for other reasons we think we can negotiate a different approach by the law enforcement agency.

Then we have to look at those relatively rare instances when we know enough, or we can discern enough to know that we have a factual basis for litigating the scope of a secrecy order. That, unfortunately, is too rare.

That's another reason why deferring this to the private sector, to the cloud providers, is not a workable solution. It's why we need to have a legislative solution that creates a greater burden on law enforcement and imposes on the judiciary the obligation to ensure that appropriate standards are met and a record of that is maintained.

Ms. BUSH. Okay. So, also considering the sheer volume of orders a provider like Microsoft can see, how burdensome is it to require providers to determine if and when each order merits a challenge? Like, tell us about that.

Mr. BURT. Well, I was asked that question earlier and I don't have specific data that I can provide about the nature of that burden.

We take it very seriously. We have a very large team that's devoted to this effort and it is constantly looking at how we can best protect our customers' rights and interests. So, it's a significant investment by Microsoft in doing this work.

I think the point for the Committee, though, is not about the burden on Microsoft. No one is going to be too sympathetic to the fact that my company has to spend money on this problem.

The problem is you should not be deferring to the private sector that responsibility, because it could vary from company to company how seriously they take this. We have only limited-visibility and limited-legal rights to challenge these secrecy orders.

We explore those rights as much as we can. You can't count on every provider doing that to the same degree or to the same extent. That's not where enforceability of these important rights should rest.

Chair NADLER. The gentlelady's time has expired.

This concludes today's hearing. Thank you to our distinguished Witnesses for participating.

Without objection, all Members will have five legislative days to submit additional written questions for the Witnesses or additional materials for the record.

Without objection, the hearing is adjourned.

[Whereupon, at 1:32 p.m., the Committee was adjourned.]