

March 20, 2017

Senator Chuck Grassley, Chairman
Senator Dianne Feinstein, Ranking Member
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Dear Chairman Grassley and Ranking Member Feinstein:

We write to you regarding the nomination of Judge Neil Gorsuch as the next Associate Justice of the Supreme Court. We urge you to explore his views on the right to privacy, on government transparency, and on the doctrines of Article III standing and *Chevron* deference. Judge Gorsuch's views on these issues could have far-reaching implications for consumer protection and the future of privacy in the digital era.

We write on behalf of the Electronic Privacy Information Center. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues.¹ We participate in a wide range of activities, including research and education, litigation, and advocacy. The EPIC Advisory Board includes leading experts in law, technology, and public policy. EPIC regularly files *amicus* briefs in the U.S. Supreme Court,² and EPIC routinely shares its views with the Senate Judiciary Committee regarding nominees to the Supreme Court.³

¹ EPIC, *About EPIC* (2017), <https://epic.org/epic/about.html>.

² See, e.g., *amicus curiae* briefs of EPIC in *Packingham v. North Carolina*, No. 15-1194 (U.S. argued Feb. 27, 2017) (arguing that the state cannot restrict the news and social media websites that a released offender may read); *Utah v. Strieff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (arguing that the violation of a consumer's privacy rights under federal law constitutes an injury-in-fact sufficient to confer Article III standing); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (arguing that hotel guest registries should not be made available for inspection absent judicial review); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that the search of a cell phone incident to arrest requires a warrant); *United States v. Jones*, 132 S. Ct. 945 (2012) (arguing that a warrant is required for the use of GPS tracking techniques); *Sorrell v. IMS Health Inc.*, 564 U.S. 52 (2011) (arguing that the privacy interest in medical records justifies regulating datamining of prescription records). See generally EPIC, *EPIC Amicus Curiae Briefs: Supreme Court* (2017), <https://epic.org/amicus/?c=Supreme+Court>.

³ See, e.g., Letter from EPIC to Senator Patrick Leahy, Chairman, & Senator Jeff Sessions, Ranking Member (June 28, 2010) (concerning the nomination of Justice Elena Kagan), https://epic.org/privacy/kagan/EPIC_Kagan_Ltr.pdf; EPIC, *1972 Alito Princeton Privacy Report* (2005), <https://www.epic.org/privacy/justices/alito/princeton/>; Letter from EPIC to Senator Arlen Specter, Chairman, & Senator Patrick Leahy, Ranking Member (Sept. 9, 2005) (concerning the nomination of Chief Justice John Roberts), <https://epic.org/privacy/justices/roberts/0905letter.pdf>.

Although EPIC takes no position for or against a judicial nominee, we urge you to scrutinize Judge Gorsuch's view on the role of the Court and Congress, privacy rights, government transparency, and judicial doctrines relevant to privacy protection.

These issues could not be more timely. The President has recently alleged that he was the target of government surveillance. Although the Chairman and Ranking Member of both the Senate and House Intelligence have found no basis to this charge,⁴ Americans are rightly concerned about the scope of surveillance, the impact of new technologies, and new business practices.⁵ They are perhaps even troubled by the prospect that the incoming administration could use the vast powers of the federal government against journalists, critics, political opponents, and others. Indeed, many of the most important privacy laws in the United States, including the Privacy Act of 1974 and the Foreign Intelligence Surveillance Act ("FISA") of 1978, came about precisely in response to the excesses of those in the White House.⁶ Critical to the effective protection of constitutional liberties and the Acts of Congress that safeguard the rights of the people is judicial independence.

The Senate Judiciary Committee should consider these issues as it begins the nomination hearings for Judge Neil Gorsuch.

Judge Gorsuch Should Be Asked About the Role of Congress and of the Court in Safeguarding Privacy

The Supreme Court has decided many important cases concerning privacy and new technologies. Recent decisions include *Riley v. California*⁷ (concerning the search of a cell phone incident to arrest) and *United States v. Jones*⁸ (concerning the attachment of a GPS tracking device to a vehicle).⁹ Several of the justices have spoken to the institutional roles that Congress and the Courts play in addressing these emerging challenges to basic freedoms.¹⁰ Justice Kagan

⁴ *Joint Statement from Senate Intel Committee Leaders on Wiretapping Evidence at Trump Tower*, U.S. Senate (Mar. 16, 2017), <http://www.warner.senate.gov/public/index.cfm/pressreleases?ID=8ABB94B7-ECC4-4E2A-9F2D-00B493295400>.

⁵ Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr. (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁶ *Privacy Act of 1974*, 5 U.S.C. § 552a, Justice Information Sharing (Aug. 16, 2013), <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>; James G. McAdams, III, Dep't of Justice, *Foreign Intelligence Surveillance Act (FISA): An Overview* (2006), https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

⁷ 134 S. Ct. 2473.

⁸ 565 U.S. 400.

⁹ See also *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (concerning whether hotel guest registries should be made available for inspection absent judicial review); *Sorrell*, 564 U.S. 52 (concerning a state law limiting the disclosure of certain types of private medical data); *Herring v. United States*, 555 U.S. 135 (2009) (concerning whether evidence obtained due to an error in a criminal justice database should be suppressed).

¹⁰ State attorneys general also play a crucial role in protecting privacy. See generally Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 748 (2016).

emphasized in a public speech that privacy “will be one of the most important issues before the Court in the decades to come.”¹¹ Justice Alito, in his concurring opinion in *Jones*, highlighted the important role that Congress plays in regulating “that complex subject” of wiretapping, noting that “concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.”¹² And Justice O’Connor wrote in a widely cited concurring opinion:

In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.¹³

Law enforcement today is presented with opportunities to use “stingray” devices, collect and test DNA samples for personal characteristics, mine social media platforms and “Big Data,” deploy drones with facial recognition, and access camera and recording devices remotely.¹⁴ The public should feel confident that Judge Gorsuch understands the role that these technologies and law enforcement techniques play in individual lives, and respects the need to govern law enforcement use of them wisely.

Given the rapid pace that technology is developing, EPIC believes it is critical for the Supreme Court, as well as Congress, to safeguard fundamental rights.¹⁵ Accordingly, the Committee should discuss with the nominee the role of the Supreme Court and of Congress in addressing the challenges that new technology presents.

Judge Gorsuch Has a Commendable Record on the Fourth Amendment

Following in the tradition of Justice Scalia, Judge Gorsuch has authored several Fourth Amendment decisions that protect individuals against intrusive searches. As a privacy organization, EPIC strongly supports constitutional limitations on the scope of government

¹¹ Tal Kopan, *Elena Kagan Talks Diversity and (Dis)agreement on the Supreme Court*, Politico (Dec. 14, 2012), <http://www.politico.com/blogs/under-the-radar/2012/12/elena-kagan-talks-diversity-and-disagreement-on-the-151963.html>.

¹² *Jones*, 565 U.S. at 427; *see also Riley*, 134 S. Ct. at 2497 (Alito, J., concurring) (“While I agree with the holding of the Court, I would reconsider the question presented here if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.”).

¹³ *Ariz. v. Evans*, 514 U.S. 1, 17–18 (1995) (O’Connor, J., concurring).

¹⁴ *See generally*; EPIC, *EPIC v. FBI - Stingray / Cell Site Simulator* (2017), <http://epic.org/foia/fbi/stingray/>; EPIC, *Genetic Privacy* (2017), <https://epic.org/privacy/genetic/>; EPIC, *Social Networking Privacy* (2016), <https://epic.org/privacy/socialnet/>; EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2017)), <https://epic.org/privacy/drones/>

¹⁵ *See* Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, 39:3 A.B.A. Hum. Rts. Mag. (2013), http://www.americanbar.org/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/protecting_privacy_courts_congress.html.

surveillance. Still, we encourage the Committee to question the nominee on several aspects of Fourth Amendment doctrine.

Search, Seizure, and New Technologies

In *United States v. Ackerman*, Judge Gorsuch authored an opinion holding that the National Center for Missing and Exploited Children (NCMEC) had violated the defendant's Fourth Amendment rights by conducting a warrantless search of his email.¹⁶ AOL, the defendant's email provider, had an automated filter which could detect images previously identified as child pornography. When that system flagged one of the defendant's emails, AOL forward the message to NCMEC. The center opened the message and established that the attachments did, in fact, contain child pornography.

Writing for the court, Judge Gorsuch determined the NCMEC, which receives funding from the government and has special powers under federal law, was a state actor. Thus, it had violated the Fourth Amendment by opening the defendant's email.¹⁷

Judge Gorsuch dissented in *United States v. Carloss*. In that case, the court determined that—despite the presence of “no trespassing” signs—police officers acted reasonably when they approached and knocked on the door of a defendant's house.¹⁸ Judge Gorsuch concluding that a reasonable officer would not have believed that they were welcome on the property and that police should have obtained a warrant. Both opinions suggest that Judge Gorsuch favors a robust interpretation of the Fourth Amendment, reflecting the intent of the framers, as did Justice Scalia.¹⁹

The Committee should ask Judge Gorsuch how the Fourth Amendment should apply in a digital context. How should the intent of the framers apply to the world of digital technology that makes possible the vast collection of personal, sensitive information? Does the advance of technology necessarily mean a diminished expectation of privacy? Will individuals have the same expectation of privacy in their digital communications as they have had in their physical communications?²⁰

¹⁶ *U.S. v Ackerman*, 831 F.3d 1292, 1308–09 (10th Cir. 2016).

¹⁷ *Id.* at 1300.

¹⁸ *United States v. Carloss*, 818 F.3d 988, 990 (10th Cir. 2016).

¹⁹ *See, e.g., Maryland v. King*, 133 S. Ct. 1958, 1989 (2011), (Scalia, J., dissenting) (“Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.”).

²⁰ *See Olmstead v. United States*, 277 U.S. 438, 475–76 (1928) (Brandeis, J., dissenting) (“The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.”).

The Committee could also ask the nominee how the Fourth Amendment doctrine may evolve as technology evolves. In *United States v. Denson*, Judge Gorsuch, writing for the majority, found that the government’s use of a radar device to determine whether someone was inside a building constituted a warrantless search under the Fourth Amendment.²¹ But in 2012, Judge Gorsuch declined to exclude evidence from a GPS device that had been placed on the defendant’s car without a warrant.²² Because police had conducted their investigation prior to the Supreme Court’s ruling that use of a GPS tracker constitutes a search,²³ the Tenth Circuit determined that officers had acted in good faith and that the GPS evidence was admissible.²⁴ That outcome was contrary to the unanimous holding of the Supreme Court in *United States v. Jones*, suggesting perhaps that Judge Gorsuch was behind the curve of the evolving doctrine of the Fourth Amendment.

The Third-Party Doctrine

EPIC also proposes that the Committee ask Judge Gorsuch about the Fourth Amendment’s “third-party” doctrine, which has diminished the privacy protections for individuals whose personal information is held by third parties, such as banks, Internet Service Providers, and medical companies.²⁵

In *Kerns v. Bader*, Judge Gorsuch, writing for the majority, determined that an officer who had requested the plaintiff’s medical records from a VA hospital had not violated the Fourth Amendment.²⁶ Judge Gorsuch applied the third-party doctrine, which dictates that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities, even if the information revealed [to the third party] on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”²⁷ This doctrine currently applies to financial information and, as Judge Gorsuch noted, “at least some courts have indicated the same analysis applies to personal medical records entrusted by patients to hospitals or care providers.”²⁸

However, the third-party doctrine is “ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”²⁹ As Justice Sotomayor has explained, even deeply private information disclosed to third parties—such as “a list of every Web site . . . visited in the last week, or month, or year”—will lack constitutional protection “unless our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.”³⁰

²¹ *United States v. Denson*, 775 F.3d 1214, 1218–19 (10th Cir. 2014).

²² *United States v. Mitchell*, 653 F. App’x 651, 653 (10th Cir. 2016).

²³ *United States v. Jones*, 565 U.S. 400 (2012).

²⁴ *Mitchell*, 653 F. App’x at 654. See generally *United States v. Knotts*, 460 U.S. 276 (1983); *United States v. Karo*, 468 U.S. 705 (1984).

²⁵ Bruce Schneier, *Data and Goliath* 67–68, 180 (2015).

²⁶ *Kerns v. Bader*, 663 F.3d 1173, 1184 (10th Cir. 2011).

²⁷ *Id.* (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)).

²⁸ *Id.*

²⁹ *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

³⁰ *Id.* at 418.

The failure of the Constitution to safeguard personal information held by third parties is an ongoing concern for many Americans and an issue that increasingly arises in federal courts.³¹ The Committee should ask Judge Gorsuch his views of the third-party doctrine and whether he believes it should be modified or eliminated.

Judge Gorsuch Has a Spotty Record on the Constitutional Right to Anonymity

The Constitution protects the right to anonymity—the right not to disclose one’s identity as a condition of exercising First Amendment freedoms.³² This right of anonymity is all the more important in the connected age: “As the means by which we can be contacted increase, so too do the means by which we can be retaliated against.”³³

The risks to anonymity arise also from new policing techniques, such as body-worn police cameras that may improve police oversight but also raise concerns about the use of techniques for mass surveillance.³⁴ For example, the constitutional right of the people to peacefully assemble and petition the government for redress of grievances is immediately implicated by police officers with body-mounted cameras moving through crowds and using facial recognition techniques to identify individuals.³⁵ Such issues are likely to be before the courts in the next few years and will require justices and judges who fully comprehend the risks to constitutional freedoms of such surveillance methods.

³¹ E.g., *In re Google Inc. Gmail Litig.*, No. 5:13-md-02430 (N.D. Cal. filed Sept. 14, 2015) (concerning Google’s interception and scanning of emails sent by non-Gmail users); *In re Facebook Biometric Information Privacy Litig.*, 3:15-cv-03747 (N.D. Cal. filed Aug. 17, 2015) (concerning Facebook’s collection and retention of facial data from user-uploaded photographs); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016 (N.D. Cal. 2014) (concerning Yahoo’s interception and scanning of emails sent by non-Yahoo Mail users).

³² *NAACP v. Alabama ex. Rel. Patterson*, 357 U.S. 449 (1958); *McIntyre*, 514 U.S. 334; *Talley v. California*, 362 U.S. 60, 64–65 (1960), *Buckley v. ACLF*, 525 U.S. 182 (1999); see also Brief of *Amicus Curiae* EPIC at 12–21, *Watchtower Bible & Tract Soc’y of New York, Inc. v. Village of Stratton*, 536 U.S. 150 (2002); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 *Stanford L. Rev.* 1373, 1425 (2000) (“The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition.”). See generally Harry Lewis, *Anonymity and Reason*, in *Privacy in the Modern Age* 104, 105–11 (Marc Rotenberg et al. eds., 2015).

³³ Brief of *Amicus Curiae* EPIC at 1–2, *Peterson v. NTIA*, 478 F.3d 626 (4th Cir. 2007) (Nos. 06–1216, 06–15480). See generally Caitriona Fitzgerald et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (EPIC 2016), <http://secretballotatrisk.org> (explaining how e-voting technology places secret ballot, and therefore right to vote anonymously, at risk).

³⁴ *Body Cameras: Can Technology Increase Protection for Law Enforcement Officers and the Public: Hearing Before the S. Judiciary Comm., Subcomm. on Crime and Terrorism* (May 19, 2015) (statement of EPIC), <https://epic.org/privacy/testimony/EPIC-Body-Camera-Statement-05-19-15.pdf>.

³⁵ Vivian Hung, Esq. et. al, *A Market Survey on Body Worn Camera Technologies* 8-404 (2016), <https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf> (“[V]endors are developing and fine-tuning next-generation BWC features such as facial recognition and weapons detection.”).

In 2010, Judge Gorsuch joined a decision by the Tenth Circuit³⁶ limiting the First Amendment right to anonymous speech.³⁷ The Utah legislature had enacted a statute requiring released sex offenders to disclose all “Internet identifiers and the addresses [used] for routing or self-identification in Internet communications”³⁸ along with the passwords for those identifiers³⁹ An offender challenged the statute on the grounds that the law unconstitutionally chilled his online speech.⁴⁰ Yet the court, including Judge Gorsuch, held that the law did “not unnecessarily interfere with his First Amendment freedom to speak anonymously.”⁴¹

Judge Gorsuch also sided with the government in two other cases concerning the compelled disclosure of identity. In 2014, the nominee wrote an opinion in a religious freedom lawsuit brought by an inmate.⁴² The plaintiff, a Muslim man who had legally changed his name for religious reasons while incarcerated, alleged that the prison officials were violating his Free Exercise rights by requiring him to list his former name when sending and receiving mail.⁴³ The court rejected the plaintiff’s challenge, concluding that the prison’s policy was “neutral toward religion and generally applicable.”⁴⁴

In 2015, Judge Gorsuch joined the Tenth Circuit’s decision in an air traveler’s lawsuit against police.⁴⁵ An Albuquerque police officer had arrested the plaintiff after he declined to stop filming at a security checkpoint and refused the officer’s demand to show identification.⁴⁶ But the court held that the officer was entitled to qualified immunity from the plaintiff’s Fourth Amendment claim, as “a reasonable officer could have believed that an investigative stop for disorderly conduct at an airport security checkpoint required the production of some physical proof of identity.”⁴⁷ The court also declined to address whether there is “First Amendment protection for creating audio and visual recordings of law enforcement officers in public places”—a right recognized by numerous other circuits.⁴⁸

³⁶ *Doe v. Shurtleff*, 628 F.3d 1217 (10th Cir. 2010).

³⁷ See *McIntyre*, 514 U.S. at 342 (“[A]n author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”).

³⁸ *Shurtleff*, 628 F.3d at 1221 (citing Utah Code Ann. § 77–27–21.5(14)(i) (West 2008)).

³⁹ *Id.* (citing Utah Code Ann. § 77–27–21.5(12)(j) & (29) (West 2008)). Identifiers used for employment or financial accounts were exempt from the law. *Id.*

⁴⁰ *Id.* at 1224.

⁴¹ *Id.* at 1225.

⁴² *Ali v. Wingert*, 569 F. App’x 562 (10th Cir. 2014).

⁴³ *Id.* at 564.

⁴⁴ *Id.* at 565.

⁴⁵ *Mocek v. City of Albuquerque*, 813 F.3d 912, 927 (10th Cir. 2015).

⁴⁶ *Id.* at

⁴⁷ *Id.* at 927.

⁴⁸ *E.g.*, *ACLU v. Alvarez*, 679 F.3d 583, 595 (7th Cir. 2012); *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000); *Fordyce v. City of Seattle*, 55 F.3d 436, 439 (9th Cir. 1995).

Judge Gorsuch's position on the right to anonymity could have significant influence on the Supreme Court, which is already considering a case about digital privacy rights under the First Amendment.⁴⁹ It would be appropriate to ask the nominee about his views on this subject.

Judge Gorsuch's Views on FOIA and Government Transparency Are Opaque

Government transparency, and in particular the Freedom of Information Act, are critical to ensuring accountability and meaningful oversight.⁵⁰ Public disclosure of government records and proceedings ensures that the nation is fully informed about the activities of the federal government. This past week Sunshine Week recognized the importance of transparency, and last year we celebrated the 50th anniversary of the FOIA and the enactment of amendments to strengthen our open government law.⁵¹

Judge Gorsuch has not authored any opinions concerning FOIA.⁵² He has joined just one Tenth Circuit opinion interpreting the statute, in which the court briefly explained that "FOIA and the Privacy Act govern document requests of federal agencies, not state agencies."⁵³

Judge Gorsuch's record is similarly limited on judicial transparency. In 2016, the nominee authored an opinion concerning civilian access to court martial proceedings. Though the plaintiffs had previously attended court martial proceedings at Fort Carson, Colorado, the base commander barred the plaintiffs from attending future hearings. The plaintiffs contended that this order interfered with their "right to observe court martial proceedings in violation of the First Amendment," an argument which Judge Gorsuch and the Tenth Circuit rejected.⁵⁴

Given Judge Gorsuch's sparse history on these issues, it would be prudent to ask him about his views on FOIA and government transparency. The Committee should question Judge Gorsuch about the excessive withholding of "working law"⁵⁵ under FOIA's deliberative process exemption,⁵⁶ the overuse of FOIA's law enforcement exemption⁵⁷ to withhold records not

⁴⁹ *Packingham v. North Carolina*, No. 15-1194 (U.S. argued Feb. 27, 2017); see also Brief of Amicus Curiae EPIC et al. in *Packingham v. North Carolina*, supra note 2.

⁵⁰ EPIC, *EPIC Open Government* (2017), https://epic.org/open_gov/.

⁵¹ EPIC, *FOIA Gallery 2016* (2016), <https://epic.org/foia/gallery/2016/>.

⁵² 5 U.S.C. § 552.

⁵³ *Jimenez v. Fourth Judicial Dist. Attorney's Office*, No. 16-1239, 2016 WL 4523971, at *3 (10th Cir. Aug. 29, 2016).

⁵⁴ *Alvarez v. Grosso*, No. 15-1398, 2016 WL 6087648, at *2 (10th Cir. Oct. 18, 2016).

⁵⁵ See, e.g., Brief for Appellant at 12, *EPIC v. Dep't of Homeland Sec.*, Nos. 13-5113, 13-5114 (D.C. Cir. voluntarily dismissed Jan. 21, 2014) ("While deliberative documents may be withheld, this privilege 'clearly has finite limits.' Materials discoverable in civil litigation are typically not protected, especially factual materials." (quoting *EPA v. Mink*, 410 U.S. 73, 87 (1973))).

⁵⁶ 5 U.S.C. § 552(b)(5).

⁵⁷ 5 U.S.C. § 552(b)(7).

connected to any specific investigation,⁵⁸ and the problem of over-classification.⁵⁹ Because these practices threaten to make FOIA “more a withholding statute than a disclosure statute,”⁶⁰ it is essential to learn the nominee’s views on them.

Judge Gorsuch’s Views on Article III Standing Are Encouraging but Not Fully Known

Article III of the Constitution grants the federal courts judicial power over “cases” and “controversies.”⁶¹ Over time, the Supreme Court has developed the doctrine of standing to ensure that federal court jurisdiction is limited “to *actual* cases or controversies.”⁶² The chief requirement of standing doctrine is that a plaintiff must have suffered an “injury-in-fact”—that is, an “invasion of a legally protected interest” which is (1) “concrete and particularized” and (2) “actual or imminent, not conjectural or hypothetical.”⁶³

In recent years, some defendants—particularly companies in privacy and consumer protection cases—have sought to manipulate standing doctrine by insisting that plaintiffs must show consequential harm above and beyond their legal injuries.⁶⁴ That pattern has continued since the Supreme Court’s recent standing decision in *Spokeo, Inc. v. Robins*,⁶⁵ which several lower courts have misread as endorsing a consequential harm theory.

This corruption of standing doctrine is deeply concerning, as it prevents plaintiffs from vindicating rights created by Congress, state legislatures, and the common law. These decisions implicate specifically the Acts of Congress that seek to protect Americans from the growing problems of data breach, identity theft, and financial fraud. Also, when a company violates consumers’ legal rights by failing to prevent a data breach of their personal information, it is often impossible for those consumers to know whether or how their data was misused by a third party. Demanding that these consumers allege some additional harm, beyond the violation of an

⁵⁸ See, e.g., Petition for Writ of Certiorari at 3, *EPIC v. Dep’t of Homeland Sec.*, No. 15-196, *cert. denied*, 136 S. Ct. 876, 877 (2016) (“[T]he Court of Appeals for the D.C. Circuit construed Exemption 7(F) so broadly that it threatens to conceal from public access all records in the possession of any federal agency upon a mere assertion that the record concerns security procedures.”).

⁵⁹ See, e.g., U.S. Dep’t of Justice Office of the Inspector Gen. Audit Div., *Audit of the Department of Justice’s Implementation of and Compliance with Certain Classification Requirements* at i (Sept. 2013) (“[O]ver-classification of information interferes with accurate and actionable information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.”); see also *Nomination Hearing for Sen. Dan Coats as Director of National Intelligence Before the S. Select Comm. on Intelligence* (Feb. 28, 2017) (statement of EPIC), <https://epic.org/testimony/congress/EPIC-SSCI-Coats-Feb2017.pdf>.

⁶⁰ *Milner v. Dep’t of Navy*, 562 U.S. 562, 565 (2011) (quoting *Mink*, 410 U.S. at 79) (quotation marks omitted).

⁶¹ U.S. Const. art. III, § 2.

⁶² *Spokeo*, 136 S. Ct. at 1547 (emphasis added).

⁶³ *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992).

⁶⁴ E.g., *Attias v. Carefirst, Inc.*, No. 16-7108 (D.C. Cir. docketed Sept. 8, 2016); *Gubala v. Time Warner Cable, Inc.*, No. 16-2613, 2017 WL 243343 (7th Cir. Jan. 20, 2017); *In re SuperValu Customer Data Security Breach Litigation*, No. 16-2378 (8th Cir. docketed May 26, 2016).

⁶⁵ 136 S.Ct. 1540 (2016).

Act of Congress, to invoke federal court jurisdiction thus bars them from seeking relief, even though they have suffered a legal injury.⁶⁶

Judge Gorsuch has not taken part in any standing cases since the *Spokeo* ruling, but his prior standing decisions suggest a relatively broad view of injury-in-fact. In 2010, he wrote that an employee of a medical practice searched by state authorities had sufficiently alleged injury-in-fact by complaining that “records from inside his personal desk were searched and seized” in violation of his “reasonable expectation of privacy in his office.”⁶⁷ Later that year, Judge Gorsuch wrote that the “out-of-pocket cost to a business of obeying a new rule of government” suffices for injury-in-fact, “whether or not there may be a pecuniary loss associated with the new rule.”⁶⁸ And in 2015, the nominee wrote that a coal company had properly alleged injury-in-fact necessary for a dormant Commerce Clause challenge where (1) the company sold coal in Colorado, and (2) the challenged state law reduced coal demand and limited the portion of the market that the company could serve.⁶⁹

Judge Gorsuch has signed on to several other notable standing decisions. In 2014, he joined the Tenth Circuit in holding that “[f]or a procedural injury, the requirements for Article III standing are somewhat relaxed, or at least conceptually expanded. . . . It suffices that the procedures are designed to protect some threatened concrete interest of [the person] that is the ultimate basis of standing.”⁷⁰ He also twice joined the court in holding that plaintiffs could establish injury-in-fact solely by alleging that their First Amendment rights had been violated.⁷¹ These cases suggest that Judge Gorsuch is willing to infer injury-in-fact even in the absence of additional harm.

Still, it is unclear whether Judge Gorsuch believes that legal injury is sufficient to confer standing in *all* cases, or whether he would graft a consequential harm requirement onto the doctrine in some instances. The Committee should question the nominee on this area of law. The standing doctrine has enormous implications for privacy protection, consumer protection, and access to the federal courts.

Judge Gorsuch Should Be Asked to Clarify His Views on Chevron Deference

EPIC urges the Committee to ask Judge Gorsuch about the *Chevron* doctrine⁷² and whether he would seek to modify it if appointed to the Court.

⁶⁶ See Brief of Amicus Curiae EPIC, *Attias v. Carefirst, Inc.* No. 16-7108 (D.C. Cir. docketed Sept. 8, 2016), <https://epic.org/amicus/data-breach/carefirst/EPIC-Amicus-Brief-Carefirst.pdf>.

⁶⁷ *Lewis v. Tripp*, 604 F.3d 1221, 1224 n.1 (10th Cir. 2010).

⁶⁸ *Hydro Res., Inc. v. EPA*, 608 F.3d 1131, 1144–45 (10th Cir. 2010).

⁶⁹ *Energy & Env't Legal Inst. v. Epel*, 793 F.3d 1169, 1175 n.1 (10th Cir.), *cert. denied*, 136 S. Ct. 595 (2015).

⁷⁰ *WildEarth Guardians v. EPA*, 759 F.3d 1196, 1205 (10th Cir. 2014).

⁷¹ *Petrella v. Brownback*, 697 F.3d 1285, 1293 (10th Cir. 2012); *Brammer-Hoelter v. Twin Peaks Charter Acad.*, 602 F.3d 1175, 1182–84 (10th Cir. 2010).

⁷² *Chevron U.S.A., Inc. v. NRDC*, 467 U.S. 837 (1984)

In *Gutierrez-Brizuela v. Lynch*, the nominee wrote a concurring opinion stating that *Chevron* “permit[s] executive bureaucracies to swallow huge amounts of core judicial and legislative power and concentrate federal power in a way that seems more than a little difficult to square with the Constitution of the framers’ design. Maybe the time has come to face the behemoth.”⁷³ Judge Gorsuch further worried that “*Chevron* invests the power to decide the meaning of the law, and to do so with legislative policy goals in mind, in the very entity charged with enforcing the law. Under its terms, an administrative agency may set and revise policy (legislative), override adverse judicial determinations (judicial), and exercise enforcement discretion (executive).”⁷⁴

The *Chevron* doctrine is one of the most significant pillars of administrative law, and changes to it could have a major impact on judicial review, consumer protection, and public safety. For example, as the Internet of Things (IoT) continues to grow and more connected devices are incorporated into everyday life, the resulting risks to consumers are also increasing.⁷⁵ EPIC has urged the Federal Trade Commission to regulate the IoT and safeguard the privacy and security of consumers and businesses.⁷⁶ If a court is asked to review a privacy-enhancing FTC action on the IoT, the vitality of the *Chevron* doctrine will be enormously consequential: will the court defer to the agency’s expertise in interpreting its Section 5 authority,⁷⁷ or will the court substitute its own reading of the statute?

Somewhat different questions arise when an agency fails to take action required by Congress. Consider, for example, the failure of the FAA to undertake a drone privacy rulemaking. Despite a mandate from Congress,⁷⁸ the Federal Aviation Administration failed to establish privacy rules for commercial drones. EPIC has petitioned the Court of Appeals for the D.C. Circuit to hold that failure unlawful,⁷⁹ given the significant risks to privacy and civil liberties of aerial surveillance, a petition to the agency for a privacy rule, and the FAA Modernization and Reform Act of 2012.⁸⁰ Were the *Chevron* doctrine revised or eliminated, the court would have a freer hand to interpret the FAA’s obligations under the 2012 law. In an earlier case, EPIC correctly argued that the TSA had failed to comply with the Administrative Procedures Act when it failed to give the public the opportunity to comment on the agency’s decision to deploy airport body scanners, which allowed agency officials to view travelers as if they were stripped naked.⁸¹

⁷³ *Gutierrez-Brizuela v. Lynch*, 834 F.3d 1142, 1149–58 (10th Cir. 2016).

⁷⁴ *Id.*

⁷⁵ EPIC, *Internet of Things (IoT)* (2017), <https://epic.org/privacy/internet/iot/>.

⁷⁶ EPIC, *Comments of the Electronic Privacy Information Center to the Federal Trade Commission on the Privacy and Security of the Internet of Things* (June 1, 2013), <https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf>.

⁷⁷ 15 U.S.C. § 45.

⁷⁸ FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 (codified at 49 U.S.C. § 40101 note).

⁷⁹ Petition for Review, *EPIC v. FAA*, No. 16-1297 (D.C. Cir. filed Aug. 22, 2016).

⁸⁰ See EPIC, *EPIC v. FAA*, <https://epic.org/privacy/litigation/apa/faa/drones/>.

⁸¹ *EPIC v DHS*, 653 F.3d. 1, 1 (D.C. Cir. 2011)

EPIC is far from alone in raising questions about Judge Gorsuch's views on *Chevron* deference.⁸² Given the implications of the *Chevron* doctrine for privacy, consumer protection, and public safety, the Committee should question the nominee extensively on this subject.

Judge Gorsuch's Should Be Asked About DNA Collection and Health Privacy

New technologies also pose significant threats to medical privacy. Methods for identification, such as rapid DNA analysis, offer the prospect of improved law enforcement. At the same time, the reliability of these techniques, as well as the equal application of these method, remains a concern.⁸³

In *United States v. Deiter*, Judge Gorsuch joined the Tenth Circuit in holding that a trial judge had not abused his discretion by refusing a criminal defendant's request to compel DNA samples from two arresting officers. The court noted that "the collection of DNA samples from the officers implicates important privacy interests."⁸⁴

We recognize the important privacy interests of law enforcement officials and at the same time are aware that there is an ongoing concern in the criminal justice system that new forensic techniques, such as DNA matching, are used almost exclusively to establish guilt and not made equally available for exculpatory purposes.⁸⁵ DNA data collection has expanded dramatically over the past decade. As of January 2017, the National DNA Index (NDIS) contains over 12,732,925 "offender" profiles, 2,608,768 arrestee profiles and 752,508 forensic profiles.⁸⁶ The profiles are heavily skewed toward low-income and minority communities.⁸⁷ In the coming years, the Supreme Court may be asked to rule on whether law enforcement can use government or private DNA databases (such as Ancestry.com) to conduct "familial searches."⁸⁸ These

⁸² E.g., Jonathan H. Adler, *Should Chevron Be Reconsidered? A Federal Judge Thinks So.*, Wash. Post (Aug. 24, 2016), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/08/24/should-chevron-be-reconsidered-a-federal-judge-thinks-so/>; Timothy B. Lee, *How Neil Gorsuch Could Rein In Regulators Like the EPA and the FCC*, Vox (Feb. 2, 2017), <http://www.vox.com/new-money/2017/2/2/14473728/neil-gorsuch-chevron-deference>.

⁸³ FBI, *Frequently Asked Questions on Rapid DNA Analysis* (2017), ("As of January 1, 2017, there is no Rapid DNA system that is approved for use by an accredited forensic laboratory for performing Rapid DNA Analysis."), <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna-analysis>.

⁸⁴ *United States v. Deiter*, 576 F. App'x 814, 816 (10th Cir. 2014). This ruling is commendable in its recognition that DNA sampling implicates serious privacy issues. To the extent that it fits a larger pattern of minimizing the importance of DNA testing of evidence when requested by a defendant, it may be troubling. See, e.g., *United States v. Roberts*, 417 F. App'x 812 (10th Cir. 2011); *Garcia v. Lind*, 574 F. App'x 857 (Mem.) (10th Cir. 2014).

⁸⁵ Erin Murphy, *Inside the Cell: The Dark Side of Forensic DNA* 149–50 (2015); see also EPIC, *Algorithms in the Criminal Justice System* (2017), <https://epic.org/algorithmic-transparency/crim-justice/>; EPIC, *Genetic Privacy* (2016), <https://epic.org/privacy/genetic/>.

⁸⁶ *CODIS - NDIS Statistics*, Fed. Bureau of Investigation (Jan. 2017), <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics>.

⁸⁷ Murphy, *supra* note 85, at 258–59; see also Shaun L. Gabbidon & Helen Taylor Greene, *Race & Crime* at Ch. 1 (4th ed. 2016), <https://books.google.com/books?id=gq1iCgAAQBAJ&pg=PT26&lpg=PT26#v=onepage&q&f=false>.

⁸⁸ Murphy, *supra* note 85, at 189–214.

searches look at DNA databases “not for the person who left the crime-scene sample, but rather for a relative of that individual.”⁸⁹ The Court may also be asked to rule on whether genetic privacy protects employees from having to choose between paying a penalty or sharing their genetic information with their employer.⁹⁰

In considering the growing use of new techniques for tracking, profiling, and matching the Committee should be aware of these developments. EPIC favors a comprehensive approach to privacy protection for new law enforcement techniques that recognizes also the risk that laws and practices may tend to favor or disfavor the rights of certain groups.

Judge Gorsuch’s early views on medical privacy are encouraging. As a student at Columbia University, he was interviewed by the *Columbia Daily Spectator* during his bid for a student council seat on whether “AIDS patients [should] be required to report their illness to the University Health Service.” Judge Gorsuch replied, “It would be, to my mind, a violation of AIDS patients’ rights and privileges of privacy to demand that they report their illness.”⁹¹

However, we are troubled by Judge Gorsuch’s more recent conclusion in *Kerns* that a police demand for medical records from a hospital did not violate the Fourth Amendment.⁹² Federal law—including HIPAA—has not protected the right to health privacy, causing the majority of the public to mistrust health technology and physicians and to withhold information from their doctors, putting their health and life at risk.⁹³ In 2002, HIPAA regulations eliminated a patient’s longstanding ethical and legal right of consent, legalizing corporate use and sales of personal data and the global health data broker industry.⁹⁴ With the public increasingly aware that their health data is not private,⁹⁵ it is critical to press Judge Gorsuch on his views concerning the future of health privacy.

Judge Gorsuch Should Be Asked About the Electronic Communications Privacy Act (“ECPA”) and Other that Safeguard Privacy

As we suggested above, privacy protections for personal communications remain a key concern for many. According to a recent survey from the Pew Research Center, “A majority of

⁸⁹ Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 Mich. L. Rev. 291, 297 (2010).

⁹⁰ Janet Burns, *GOP Bill Could Force Employees To Undergo DNA Tests Or Pay Huge Fines* (Mar. 14, 2017), <https://www.forbes.com/sites/janetwburns/2017/03/14/gop-bill-could-force-employees-to-undergo-dna-testing-or-pay-thousands/#48a6b2aa71fe>.

⁹¹ *At-Large Candidates*, Colum. Daily Spectator, Mar. 19, 1986, at 7, 12, <http://spectatorarchive.library.columbia.edu/cgi-bin/columbia?a=d&d=cs19860319-01.1.11&e=-----en-20--1--txt-txIN-%22Neil+Gorsuch%22+%26+privacy-----#>.

⁹² 663 F.3d at 1184.

⁹³ Black Book Market Research, *Healthcare’s Digital Divide Widens, Black Book Consumer Survey* (Jan. 3, 2017), <https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252>.

⁹⁴ Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,183 (Aug. 14, 2002) (to be codified at C.F.R. pts. 160, 164); see also Mark A. Rothstein & Laura Rothstein, *How Genetics Might Affect Real Property Rights*, J. L. Med. & Ethics, Spring 2016, at 216, 216–221.

⁹⁵ Black Book Market Research, *supra* note 93.

Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions—especially the federal government and social media sites—to protect their personal information.”⁹⁶

Under the Electronic Communications Privacy Act, the government may demand stored communications and transaction records from third-party service providers simply by offering “specific and articulable facts showing that there are reasonable grounds to believe that the ... records or other information sought[] are relevant and material to an ongoing criminal investigation.”⁹⁷ This is a markedly lower standard than the showing of probable cause required for a warrant.

On two occasions,⁹⁸ Judge Gorsuch has rejected the argument that a government violation of ECPA warrants the exclusion of the resulting evidence—the same remedy that would ordinarily be available for a Fourth Amendment violation. “Subscriber information provided to an Internet service provider is not protected by the Fourth Amendment's privacy expectation,” Judge Gorsuch wrote in *United States v. Swenson*.⁹⁹ “Neither do violations of the Electronic Communications Act warrant exclusion of evidence.”¹⁰⁰ The Committee should ask Judge Gorsuch whether he believes that ECPA offers sufficient privacy protections for emails and other stored communications, particularly if individuals lack a remedy for unlawful searches.

* * *

Finally, we note with concern the treatment of Chief Judge Merrick Garland by the Committee and the United States Senate. Judge Garland was nominated by President Obama to the U.S. Supreme Court on March 15, 2016. Judge Garland is one of the preeminent jurists in the country, known for his thoughtfulness, collegiality, and moderate views. President Obama said of Judge Garland, he “is widely recognized not only as one of America’s sharpest legal minds, but someone who brings to his work a spirit of decency, modesty, integrity, even-handedness, and excellence.”¹⁰¹

For 293 days, the nomination of Judge Garland was pending before the Senate. Yet, no hearing was ever held. No vote was ever taken. He was never even given the opportunity to appear before the Committee. The nomination simply expired on January 3, 2017.¹⁰²

⁹⁶ Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Res. Ctr. (Jan. 26, 2017), <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>.

⁹⁷ 18 U.S.C. § 2703(d).

⁹⁸ *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (holding that violations of the ECPA do not warrant exclusion of evidence); *United States v. Swenson*, 335 F. App'x 751, 754 n.1 (10th Cir. 2009) (same).

⁹⁹ *Swenson*, 335 F. App'x at 754 n.1.

¹⁰⁰ *Id.*

¹⁰¹ Michael D. Shear, Julie Hirschfield Davis, & Gardiner Harris, *Obama Chooses Merrick Garland for Supreme Court*, N.Y. Times (Mar. 16, 2016), <https://www.nytimes.com/2016/03/17/us/politics/obama-supreme-court-nominee.html>.

¹⁰² Jess Bravin, *President Obama's Supreme Court Nomination of Merrick Garland Expires: Garland's nomination languished for 293 days as Republicans declined to give him a hearing*, Wall Street J. (Jan. 3,

The Senate’s refusal to act on the nomination of Judge Garland was an abdication of constitutional responsibility by the “world’s greatest deliberative body,”¹⁰³ and of concern to groups such as EPIC that participate in the work of the Court.

As Judge Gorsuch has himself lamented, “The judicial confirmation process today bears no resemblance” to the confirmations of 50 years ago.¹⁰⁴ “Today, there are too many who are concerned less with promoting the best public servants and more with enforcing litmus tests and locating unknown ‘stealth candidates’ who are perceived as likely to advance favored political causes once on the bench. . . . Whatever else might be said about the process today, excellence plainly is no longer the dispositive virtue.”¹⁰⁵ Judge Gorsuch has even expressed frustration at how Chief Judge Garland—one of the “finest lawyers of [his] generation”—was “mistreated” during his lengthy nomination process for the D.C. Circuit.¹⁰⁶

Given that Judge Gorsuch has expressed views on the nomination process and the qualifications of Chief Judge Merrick Garland, he could be asked about the Senate’s handling of Judge Garland’s nomination.

We ask that this letter from EPIC be entered into the hearing record.

As always, EPIC appreciates your consideration of our views and would be pleased to provide the Senate Judiciary Committee with any additional information you request.

Sincerely,

Marc Rotenberg
President, EPIC

Steven Aftergood
Project Director, Federation of American Scientists

Anita Allen,
Vice Provost for Faculty, University of Pennsylvania

James Bamford
Author

2017), <https://www.wsj.com/articles/president-obamas-supreme-court-nomination-of-merrick-garland-expires-1483463952>.

¹⁰³ Paul Kane, *On the death of the Senate and its long history as the world’s greatest deliberative body*, Wash. Post (Jan. 31, 2017), https://www.washingtonpost.com/powerpost/on-the-death-of-the-senate-and-its-long-history-as-the-worlds-greatest-deliberative-body/2017/01/31/b99fcbda-e73a-11e6-bf6f-301b6b443624_story.html.

¹⁰⁴ Neil Gorsuch, *Justice White and judicial excellence*, UPI (May 4, 2002), <http://www.upi.com/Justice-White-and-judicial-excellence/72651020510343/>.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

Ann Bartow
Professor, Pace Law School

Francesca Bignami
Professor of Law, George Washington University School of Law

Christine L. Borgman,
*Distinguished Professor and Presidential Chair in Information Studies,
UCLA; Director, UCLA Center for Knowledge Infrastructure*

Ryan Calo
Assistant Professor, University of Washington School of Law

David Chaum
Chaum, LLC

Danielle Keats Citron
*Morton & Sophia Macht Professor of Law, University of Maryland School
of Law*

Julie E. Cohen
*Professor, Director of the Center on Privacy and Technology,
Georgetown University Law Center*

Dr. Whitfield Diffie
*Consulting Scholar, Stanford Center for International Security and
Cooperation*

Cynthia Dwork
*Gordon McKay Professor of Computer Science, Radcliffe Alumnae
Professor at the Radcliffe Institute for Advanced Study, and Affiliated
Professor, Harvard Law School.*

David J. Farber
*Distinguished Career Professor of Computer Science and Public Policy,
Carnegie Mellon University*

Philip Friedman
Executive Director, Consumers Count

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya
Professor of Computer Science, Brown University

Aleecia M. McDonald
Non-resident fellow, Stanford Center for Internet and Society

Mary Minow
Library Law Consultant

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Erin Murphy
Professor of Law, New York University

Dr. Peter G. Neumann
Computer Science Laboratory, SRI International

Helen Nissenbaum
Professor, Director of the Information Law Institute, New York University

Dr. Cathy O'Neil
Founder, O'Neil Risk Consulting and Algorithmic Auditing

Dr. Deborah Peel, M.D.
Founder and Chair, Patient Privacy Rights

Ronald L. Rivest
Professor of Electrical Engineering and Computer Science, MIT

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law, Berkeley Law School

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Dr. Barbara Simons
Founder and Former Chair, USACM, the ACM U.S. Public Policy Committee

Robert Ellis Smith
Publisher, Privacy Journal

Frank Tuerkheimer
Professor of Law Emeritus, University of Wisconsin Law School

Sherry Turkle
*Abby Rockefeller Mauzé Professor of the Social Studies of Science and
Technology, MIT*

James Waldo
Gordon McKay Professor of the Practice of Computer Science

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff
*Charles Edward Wilson Professor of Business Administration (emeritus),
Harvard Business School*

(Affiliations are for identification only.)