



DIVISION OF
CORPORATION FINANCE

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

January 30, 2017

Wayne Wirtz
AT&T Inc.
wayne.wirtz@att.com

Re: AT&T Inc.
Incoming letter dated December 6, 2016

Dear Mr. Wirtz:

This is in response to your letters dated December 6, 2016 and January 19, 2017 concerning the shareholder proposal submitted to AT&T by Benjamin Ewen-Campen. We also have received a letter on the proponent's behalf dated January 6, 2017. Copies of all of the correspondence on which this response is based will be made available on our website at <http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8.shtml>. For your reference, a brief discussion of the Division's informal procedures regarding shareholder proposals is also available at the same website address.

Sincerely,

Matt S. McNair
Senior Special Counsel

Enclosure

cc: Pat Miguel Tomaino
Zevin Asset Management, LLC
pat@zevin.com

January 30, 2017

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: AT&T Inc.
Incoming letter dated December 6, 2016

The proposal asks the board to review and publicly report on the consistency between the company's policies on privacy and civil rights and the company's actions with respect to U.S. law enforcement investigations.

There appears to be some basis for your view that AT&T may exclude the proposal under rule 14a-8(i)(7), as relating to AT&T's ordinary business operations. In this regard, we note that the proposal relates to procedures for protecting customer information. Accordingly, we will not recommend enforcement action to the Commission if AT&T omits the proposal from its proxy materials in reliance on rule 14a-8(i)(7). In reaching this position, we have not found it necessary to address the alternative basis for omission upon which AT&T relies.

Sincerely,

Mitchell Austin
Attorney-Adviser

DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the company in support of its intention to exclude the proposal from the company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes and rules administered by the Commission, including arguments as to whether or not activities proposed to be taken would violate the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversarial procedure.

It is important to note that the staff's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly, a discretionary determination not to recommend or take Commission enforcement action does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the company's management omit the proposal from the company's proxy materials.



Wayne Wirtz
Vice President and
Associate General Counsel

AT&T Inc.
One AT&T Plaza
208 S. Akard Street
Dallas, TX 75202

T: 214.757.3344
F: 214.746.2273
wayne.wirtz@att.com

1934 Act/Rule 14a-8

January 19, 2017

By email: shareholderproposals@sec.gov

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: 2017 AT&T Inc. Annual Meeting of Shareholders – Supplemental
Request to Exclude Shareholder Proposal of Benjamin Ewen-Campen
Pursuant to Rule 14a-8

Ladies and Gentlemen:

Zevin Asset Management, LLC on behalf of Benjamin Ewen-Campen (the “Proponent”) submitted a shareholder proposal and statement in support thereof (collectively, the “2017 Proposal”) to AT&T Inc. (“AT&T” or the “Company”) for inclusion in AT&T’s proxy statement and form of proxy for its 2017 Annual Meeting of Shareholders (collectively, the “2017 Proxy Materials”). The 2017 Proposal requests that the Board “review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on the consistency between AT&T’s policies on privacy and civil rights and the Company’s actions with respect to U.S. law enforcement investigations. This proposal addresses programs in use domestically like *Hemisphere*.”

This supplemental letter is submitted in response to a letter from the Proponent, dated January 6, 2017 (the “January 6 Response”), and should be read in conjunction with AT&T’s December 6, 2016 letter to the Staff, notifying it of AT&T’s intent to exclude the 2017 Proposal pursuant to Exchange Act Rule 14a-8 (the “December 6 Submission”).

ARGUMENT

To avoid the conclusion that the 2017 Proposal is substantially similar to a proposal received by AT&T last year (the “2016 Proposal”),¹ and is therefore excludable

¹ See *AT&T Inc.* (Feb. 5, 2016).

pursuant to Rule 14a-8(i)(7), the January 6 Response draws a puzzling distinction between the 2017 Proposal and the 2016 Proposal. It asserts that, unlike the 2016 Proposal, “this Proposal does not focus on Company ‘policies’” concerning privacy.² That purported distinction is obviously in tension with the language of the 2017 Proposal itself as well as the balance of the January 6 Response, which reiterates the request for the Company to issue a report concerning potential “inconsistencies between the Company’s approach to the issue of telecommunications privacy” and certain law enforcement programs. The January 6 Response then goes on to say, “[t]o address those inconsistencies, the Proposal necessarily raises AT&T’s privacy policies, but it does not prescribe, dictate or otherwise interfere with the company’s policies or their disclosure.”³ How the 2017 Proposal can both avoid focusing on AT&T’s privacy-related policies and yet seek a report on AT&T’s “approach” to privacy in a way that “necessarily raises AT&T’s privacy policies” is unclear.

Indeed, the 2016 Proposal included a substantively identical request, namely that the Company “issue a report... clarifying the Company’s policies regarding providing information to law enforcement,” including by addressing purported “AT&T behavior that appear[s] inconsistent with its pledge to protect privacy...”⁴ If there is any distinction between the report sought by the 2017 Proposal and the report sought by the 2016 Proposal, it is a distinction without a difference.

And in fact, there is no meaningful distinction. Like the 2016 Proposal, the 2017 Proposal focuses on matters of ordinary business, including the Company’s policies and procedures for protecting privacy. AT&T’s legal compliance program with respect to providing information to law enforcement agencies is also a matter of ordinary business. Importantly, it is not the Company that makes a “policy decision to design, launch, and potentially expand a program like *Hemisphere*,” a flatly inaccurate statement made in the January 6 Response.⁵ *Hemisphere* is a government program, its design and scope are determined by governmental authorities, and AT&T has a legal compliance program in place in response to authorized intelligence and law enforcement efforts. That significant misstatement notwithstanding, the Company’s Transparency Reports already provide extensive disclosure of the nature contemplated by the 2017 Proposal, including an outline of its legal compliance program and descriptions of the Company’s procedures for responding to various types of demands for information from law enforcement and intelligence agencies.⁶

² See January 6 Response at 4.

³ See *id.*

⁴ See *AT&T Inc.* (Feb. 5, 2016).

⁵ See January 6 Response at 8.

⁶ The Transparency Reports are available at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>. Among its other disclosures, the Company has consistently and publicly articulated that, in connection with its legal compliance program, it discloses information outside

CONCLUSION

The Company, therefore, stands on the December 6 Submission and this supplemental letter for the reasons stated above. Accordingly, the Company continues to believe that the Proposal may be excluded from its 2017 Proxy Materials pursuant to Rule 14a-8(i)(7) and Rule 14a-8(i)(10).

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

Sincerely,

A handwritten signature in black ink that reads "Wayne Wirtz". The signature is written in a cursive style and is contained within a light gray rectangular box.

Wayne Wirtz

cc: Pat Miguel Tomaino, Zevin Asset Management, LLC

of the Company under certain circumstances to intelligence and law enforcement officials in order to “[c]omply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements... [or] [n]otify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury.” See AT&T Privacy Policy, available at https://about.att.com/sites/privacy_policy/full_privacy_policy.

Zevin Asset Management, LLC

PIONEERS IN SOCIALLY RESPONSIBLE INVESTING

January 6, 2017

Via E-Mail: shareholderproposals@sec.gov

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: AT&T, Inc. December 6, 2016 Request to Exclude Shareholder Proposal Regarding Telecommunications Privacy and *Hemisphere*

Ladies and gentlemen:

This letter is submitted on behalf of Benjamin Ewen-Campen by Zevin Asset Management, LLC as the designated representative in this matter (hereinafter referred to as “Proponent”), who is the beneficial owner of 1,900 shares of common stock of AT&T, Inc. (hereinafter referred to as “AT&T” or the “Company”), and who has submitted a shareholder proposal (hereinafter referred to as “the Proposal”) to AT&T, to respond to the letter dated December 6, 2016 sent to the Office of Chief Counsel by AT&T, in which it contends that the Proposal may be excluded from the Company's 2017 proxy statement under Rule 14a-8(i)(7) and Rule 14a-8(i)(10).

After reviewing the Company's letter and the relevant SEC rules as they apply to the Proposal, we have concluded that the Proposal must be included in AT&T's 2017 proxy statement, because the Proposal raises and focuses on a significant policy issue confronting AT&T and the Company has not substantially implemented the Proposal. Therefore, we respectfully request that the Staff not issue the no-action letter sought by the Company.

Pursuant to Staff Legal Bulletin 14D (November 7, 2008) we are filing our response via e-mail in lieu of paper copies, and we are providing a copy to AT&T's Associate General Counsel and Assistant Secretary, Wayne Wirtz via e-mail at ww0118@att.com.

I. The Proposal

The Proposal reads as follows:

Whereas: There is widespread public debate about how cooperation between U.S. law enforcement entities and telecommunications companies affects Americans' privacy and civil rights.

Senator Edward Markey, one of many policymakers calling for regulators to review AT&T's proposed acquisition of Time Warner, remarked in October 2016: “We need a telecommunications market...where our right to privacy is maintained even when technologies change.”

AT&T's Privacy Policy indicates the Company seeks to protect customer information and privacy while complying with applicable law. The July 2016 Transparency Report states:

“Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements.”

However, the above guidance, which indicates a cautious approach to cooperating with law enforcement agencies, is at odds with AT&T’s vast *Hemisphere* program.

Revealing details of *Hemisphere* in 2013, *The New York Times* reported that local and federal law enforcement agencies “had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans’ phone calls.”

According to that report, “[t]he government pays AT&T to place [AT&T] employees in drug-fighting units around the country” and “[t]he Obama administration acknowledged the extraordinary scale of the *Hemisphere* database and the unusual embedding of AT&T employees in government drug units in three states.”

In October 2016, we learned that AT&T positioned *Hemisphere* as a lucrative product aimed at a wide range of agencies and investigations. *The Daily Beast* reported: “Sheriff and police departments pay from \$100,000 to upward of \$1 million a year or more for *Hemisphere* access.”

Several additional aspects of *Hemisphere* appear to go above and beyond legal requirements:

- *Hemisphere* is an extraordinarily large database going back as far as 1987, according to *The New York Times*. Other reports indicate AT&T’s cellular tower data retention exceeds that of peer companies like Verizon and Sprint.
- AT&T hides *Hemisphere* by apparently requiring agencies not to use *Hemisphere* data in court unless no other evidence is available.
- *Hemisphere*’s size and AT&T’s decision to offer forms of analysis which connect call records and phones to each other enable searches which would not otherwise occur.

Hemisphere and AT&T’s involvement in it have prompted questions from legal experts and widespread attention from global media outlets including *The Wall Street Journal*, *Guardian*, and *Breitbart*.

While AT&T must follow the law, shareholders are concerned that failure to persuade customers of a consistent and long-term commitment to privacy rights could present serious financial, legal, and reputational risks.

Resolved: Shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on the consistency between AT&T’s policies on privacy and civil rights and the Company’s actions with respect to U.S. law enforcement investigations. This proposal addresses programs in use domestically like *Hemisphere*. It does not request information on international activity, national security, nor disclosures that would violate any laws.

II. The Proposal is Focused on Telecommunications Privacy, Which is Not an Ordinary Business Matter

AT&T's *Hemisphere* program has caused concern among both the public and investors and highlights the need for new disclosure. To summarize briefly, reports indicate that AT&T maintains an extraordinarily large database of call data. According to those reports, the Company sells access to that database to local, state, and federal law enforcement agencies for fees as high as \$1 million per year. That process, which is described as the *Hemisphere* program, reportedly entails: customized searches conducted by AT&T for law enforcement agencies, the embedding of AT&T employees in law enforcement agencies, and high levels of secrecy required by AT&T.

Programs like *Hemisphere* raise concern about the Company's approach to telecommunications privacy. This Proposal is focused on the broad issue of telecommunications privacy, and in Section III we will substantiate that telecommunications privacy is a significant policy issue subject to widespread public debate and examination.

At the outset, however, we wish to note that the Proposal addresses its focus — telecommunications privacy — while avoiding micro-management or prying into day-to-day business operations. Contrary to AT&T's contentions, the Proposal does not interfere with the Company's policies or procedures "for protecting customer information" nor "the conduct of its legal compliance program."

In arguing that the Proposal interferes with policies and procedures "for protecting customer information" and legal compliance the Company relies on the notion that the Proposal is similar to a 2016 resolution proposed by Arjuna Capital (hereafter referred to as the "Arjuna proposal"). To state the obvious, this Proposal is distinct from the Arjuna proposal, with a distinct request in the Resolved clause and different motivating concerns detailed in the Whereas clauses. While the Arjuna proposal asked for reporting on Company conduct "above and beyond what is legally required by court order or other legally mandated process," this Proposal queries the consistency between AT&T's actions and the "policies on privacy and civil rights" that the Company has set for itself. Whereas the Arjuna proposal inquired about data requests from intelligence agencies, this Proposal is specifically focused on the Company's actions with respect to investigations carried out by local, federal and state law enforcement agencies in the U.S. To state the even more obvious, Arjuna Capital is not a proponent of this Proposal and has not co-filed this Proposal.

A. The Proposal Does Not Interfere with Customer Privacy Policies or Procedures

The Company's focus on the Arjuna proposal (and its permitted exclusion last year) is unconvincing because this Proposal does not interfere with or focus on the Company's procedures or policies. Rather, the Proposal is focused on disclosure of potential gaps between AT&T's decision to offer *Hemisphere* and the Company's overall approach to telecommunications privacy as reasonably perceived by outside stakeholders based on the Company's own policies.

In assessing the Proposal's approach to AT&T's policies, we invite the Staff to consider its recent decision refusing to exclude a proposal at CVS Health Corporation which asked for the company to examine the congruency between professed "corporate values" and certain actions of the company. Such requests, which compare policies regarding significant policy issues with actual

implementation, are appropriate for investor concern and beyond ordinary business matters (*CVS Health Corp*, February 9, 2015).¹

i. Policies

Unlike the Arjuna proposal, which could conceivably be construed as requesting the disclosure or formulation of privacy policies covering law enforcement requests, this Proposal does not focus on Company “policies.” Rather, this Proposal queries the distance and inconsistencies between the Company’s approach to the issue of telecommunications privacy and programs like *Hemisphere*. To address those inconsistencies, the Proposal necessarily raises AT&T’s privacy policies, but it does not prescribe, dictate or otherwise interfere with the company’s policies or their disclosure.

AT&T has extensive policies that project to customers, investors, and the public (collectively, “outside stakeholders”) that privacy is an integral part of its social responsibility. For instance, AT&T’s general Privacy Commitments begins by stating:

“Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.”²

The first of AT&T’s Privacy Commitments states:

We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.³

The company’s July 2016 Transparency Report states:

Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid, and that our responses comply with the law and our own policies.⁴

When *The Daily Beast* approached AT&T for comment about the *Hemisphere* program in October, 2016, the Company supplied stated:

“Like other communications companies, if a government agency seeks customer call records through a subpoena, court order or other mandatory legal process, we are required by law to provide this non-content information, such as the phone numbers and the date and time of calls[.]”⁵

¹ <https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2015/northstarasset020915-14a8.pdf>

² https://about.att.com/sites/privacy_policy

³ Ibid.

⁴

https://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf

⁵ <http://www.thedailybeast.com/articles/2016/10/25/at-t-is-spying-on-americans-for-profit.html>

Those policies and statements shape outside stakeholders' impression of AT&T's general approach to telecommunications privacy — both (1) their understanding of AT&T's position on the issue and (2) their expectations about the actions that AT&T will generally take with respect to the issue.

This Proposal does not seek further explication of these policies or the development of new policies regarding telecommunications privacy. Rather, the Proposal presents investors' concern that the reported operation of *Hemisphere* is inconsistent with the understandings and expectations created by those policies.

In the Proponent's view, AT&T's privacy policies invite outsiders to form the overall impression that the Company complies with all lawful requests from agencies, but that it takes a cautious and conservative approach to fulfilling requests and it cooperates with domestic law enforcement investigations only as far as it takes to follow the law. The Proposal raises the concern that *Hemisphere's* reported scope, customization of searches, secrecy, and commercialization all conflict with that reasonably-formed impression of AT&T's approach to telecommunications privacy.

That potential inconsistency is important because customers, investors, and the public care about AT&T's general approach to telecommunications privacy. In developing and publishing certain privacy policies over the years, AT&T has conceded as much. That outsiders care about AT&T's approach to telecommunications privacy is confirmed by surveys showing that 90 percent of Americans report that "controlling what information is collected about them is important" and 93 percent say that "being in control of *who* can get information about them is important."⁶

Americans' concerns about telecommunications privacy are further demonstrated by the widespread public debate and examination of the issue which will be further detailed in Section III. We raise the issue here, however, to emphasize investors' sincere and legitimate concern over the distance between outside stakeholders' impression of AT&T's approach to telecommunications privacy and reported features of *Hemisphere*. After all, if customers perceive that the Company's actions or products contradict the impression invited by its privacy policies, they may punish AT&T in the marketplace. Policymakers may punish AT&T in the legislative or regulatory process. Both situations are concerning for the company and its investors.

Given that the Proposal is focused on the distance between stakeholders' impressions of its policies and its reported actions, the Company need not formulate new policies nor make new disclosures of existing policies to respond to the Proposal's request ("report...on the consistency between AT&T's policies on privacy and civil rights and the Company's actions with respect to U.S. law enforcement investigations").

To address investors' concerns, the company might simply disclose or amend its current disclosures to include information about programs like *Hemisphere* in light of its existing privacy policies. As indicated by the Resolved clause of the Proposal, these disclosures would be undertaken "at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information" and without violating any laws. (In its letter, the Company does not contend that such disclosure would be unreasonable in any of these respects.)

ii. Procedures

⁶ <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>

The Company is even farther off base in its contention that the Proposal seeks to dictate or micro-manage “procedures for protecting customer information.” The words “procedure” or “procedures” do not appear anywhere in the Proposal, nor is the concept invoked.

The proposal does not focus on or inquire into the Company’s specific procedures for protecting customer privacy when presented with law enforcement requests or in any other situations. Rather, the Proposal raises concerns about the consistency between the impressions that reasonable outsiders would form of AT&T’s approach to telecommunications privacy and *a service (“Hemisphere”) which reflects its actual approach to telecommunications privacy*. To do that, the Proposal necessarily mentions specific reported features of *Hemisphere*, which, according to news reports, may run against outside stakeholders’ understandings and expectations:

- ***Hemisphere is reportedly expansive.*** According to *The New York Times*, *Hemisphere* provides access to an extraordinarily large database going back as far as 1987.⁷ *The Daily Beast* reported: “AT&T retains its cell tower data going back to July 2008, longer than other providers. Verizon holds records for a year and Sprint for 18 months...”⁸
- ***Hemisphere reportedly enables customized, advanced call data searches.*** According to the *Daily Beast* report, the large size of AT&T’s database “allows its analysts to detect hidden patterns and connections between call detail records.” Reportedly, this allows law enforcement searching *Hemisphere* to track “a subscriber between multiple discarded phone numbers, as when drug dealers use successive prepaid ‘burner’ phones to evade conventional surveillance.” The advanced functionality of *Hemisphere* searches also reportedly enables agencies to “make highly accurate inferences about the associations and movements of the people *Hemisphere* is used to surveil.” Conceivably, this helps law enforcement agencies retrieve the data of people not named in the original search.⁹
- ***Hemisphere is reportedly secretive.*** According to the above-cited *Daily Beast* report, AT&T hides *Hemisphere* by apparently requiring agencies not to use *Hemisphere* data in court unless no other evidence is available.¹⁰
- ***Hemisphere has apparently been commercialized.*** According to the above-cited *Daily Beast* report, “*Hemisphere* isn’t a ‘partnership’ but rather a product AT&T developed, marketed, and sold at a cost of millions of dollars per year to taxpayers.” Citing a contract that it obtained, *The Daily Beast* reported that “Sheriff and police departments pay from \$100,000 to upward of \$1 million a year or more for *Hemisphere* access. Harris County, Texas, home to Houston, made its inaugural payment to AT&T of \$77,924 in 2007...[,] Four years later, the county’s *Hemisphere* bill had increased more than tenfold to \$940,000.”¹¹

The reported element of commercialization is particularly at odds with stakeholders’ understanding and expectations of AT&T’s approach to telecommunications privacy. Historically, telecommunications companies have provided law enforcement with access to

⁷ <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>

⁸ <http://www.thedailybeast.com/articles/2016/10/25/at-t-is-spying-on-americans-for-profit.html>

⁹ Ibid.

¹⁰ Ibid.

¹¹ Ibid.

data and metadata on an at-cost basis. However, according to a 2013 *Associated Press* report, there is evidence that the prices companies charge government agencies for carrying out mandated surveillance functions have increased. According to that report, there is a risk that surveillance could become a profit center for telecommunications companies as prices rise, ultimately leading to “uncalled-for surveillance.”¹²

Reports that AT&T has decided to charge close to \$1 million for *Hemisphere* — conceivably in multiple jurisdictions throughout the U.S. — invite speculation that domestic surveillance cooperation at AT&T is dangerously close to being commercialized.

These reported features of *Hemisphere* run directly counter to the impressions outside stakeholders might reasonably form from AT&T’s own policies, namely that the company has a cautious, even conservative, approach to domestic law enforcement investigations.

This Proposal assumes that AT&T’s decision to offer *Hemisphere* as reported reflects the company’s actual approach to the policy matter of telecommunications privacy. That policy decision and its potential conflicts with the Company’s perceived overall approach to the issue of telecommunications privacy form the focus of the Proposal, not any particular operative details or “procedures.” The commercialization aspect of *Hemisphere* and other concerning reported features of the program are cited only in an attempt to characterize *Hemisphere* and AT&T’s decision to offer the program. The Proposal’s discussion of particular features of *Hemisphere*, therefore, does not dictate or interfere with the Company’s “procedures for protecting customer information.”

Thus, the Company is mistaken in its assertion that the Proposal interferes with or seeks to micro-manage its policies and procedures. Disclosures about reported AT&T actions as they relate to existing privacy policies would address investor concerns about the distance between AT&T’s actions and the impressions that outside stakeholders might reasonably draw from the Company’s own pronouncements. A request for this kind of disclosure was blessed by the Staff in *CVS Health Corp* (2015), cited above.

Within the reasonable constraints discussed above (cost, timing, confidentiality, legal compliance, etc.) a report could discuss the way in which such programs might be in tension with telecommunications privacy, along with the Company’s thoughts on resolving those conflicts. The only conceivable way in which such disclosures would invade the Company’s “ordinary business” would be if the Company believed that breaching the privacy of the people who use its networks is its “ordinary business.” And that is simply not the case.

iii. The “Nitty Gritty”

Because the Proposal queries the Company’s general approach to telecommunications privacy, it does of course touch on privacy, the Company’s customers, and its various procedures. However, the Staff has clearly indicated, a company may not exclude proposals merely because the proposals may relate to the “nitty-gritty of its core business.” Indeed, “proposals focusing on a significant policy issue are not excludable under the ordinary business exception” because those proposals

¹² <http://www.usatoday.com/story/money/business/2013/07/10/what-government-pays-to-snoop-on-you/2504819/>

would necessarily “transcend a company’s ordinary business operations” (Staff Legal Bulletin 14H (October 22, 2015) (internal citations omitted) (“SLB 14H”).

Viewed from this perspective, the fact that the Proposal might in some sense *relate to* the Company’s decisions regarding protecting customer information is not sufficient to exclude it. Rather, the Company must additionally show that the Proposal does not focus on a significant policy issue.

B. The Proposal Does Not Focus on Matters of Legal Compliance

Without belaboring the points raised above, we would re-emphasize that this Proposal is focused on disclosure of potential gaps between AT&T’s decision to offer *Hemisphere* and the Company’s overall approach to telecommunications privacy as reasonably perceived by outside stakeholders based on the Company’s own policies.

The Proposal does not impermissibly focus on the Company’s legal compliance programs. Although the Proposal addresses the issue of telecommunications privacy, the Proposal does not inquire as to mechanisms or strategies that the Company utilizes to engage in legal compliance matters. On the contrary, disclosures that would be responsive to this Proposal would include information on *Hemisphere* (and/or programs like it) in light of the Company’s existing privacy policies. Again, the focus of such reporting would be any potential inconsistencies between those programs and impressions of the Company’s approach to telecommunications privacy — not inconsistencies between *Hemisphere* and applicable law.

Because the Proponent desired to avoid interfering with matters of legal compliance, the Proposal specifically invites the Company to omit, at its discretion, “proprietary and confidential information” as well as any “information on international activity, national security, nor disclosures that would violate any laws.”

When and how the Company decides to turn over data in response to requests from law enforcement agencies is an operational matter lying somewhat beneath the concerns of this Proposal. Rather, this Proposal examines the Company’s policy decision to design, launch, and potentially expand a program like *Hemisphere*. Querying the risks of such programs does not impugne or invade the Company’s legal compliance.

In sum, the Proposal does not, as AT&T argues, focus on policies or procedures “for protecting customer information” or on the “conduct of [AT&T’s] legal compliance program. Instead, the Proposal seeks additional information on the broad matter of AT&T’s approach to telecommunications privacy and how the reasonably-formed impressions of AT&T’s stakeholders may be in conflict with programs like *Hemisphere*.”

The Company has not shown that the Proposal invades its ordinary business.

III. Telecommunications Privacy is a Significant Policy Issue

A shareholder proposal generally may not be excluded under Rule 14a-8(i)(7) when “a proposal’s underlying subject matter transcends the day-to-day business matters of the Company and raises policy issues so significant that it would be appropriate for a shareholder vote.” (Staff Legal Bulletin 14E (October 27, 2009)). According to the Staff, “the presence of widespread public debate regarding an issue is among the factors to be considered in determining whether proposals

concerning that issue ‘transcend the day-to-day business matters’” (Staff Legal Bulletin 14A (July 12, 2002) (internal citation omitted)).

As noted above, proposals dealing with significant policy issues will not be excludable simply because they may relate to the “nitty-gritty of [the Company’s] core business.” Rather, proposals judged to focus on significant policy issues necessarily “transcend a company’s ordinary business operations and are not excludable under Rule 14a-8(i)(7)” (SLB 14H).

Finally, the Company bears the burden of persuasion on this question (Rule 14a-8(g)). The SEC has made it clear that under the Rule “the burden is on the company to demonstrate that it is entitled to exclude a proposal.” Exchange Act Release No. 34-40018 (May 21, 1998) (“1998 Interpretive Release”)

Telecommunications privacy is very clearly a significant policy issue. This is evidenced in widespread public examination and debate of the issue among scholars, policymakers, activists, customers, and the general public.

In attempting to resist shareholder proposals related to telecommunications privacy in the past, we must note that AT&T has been allowed to constrain the scope of this significant policy issue. In its request to exclude a proposal on semi-annual transparency reporting filed by The New York State Common Retirement Fund for the 2014 annual meeting of stockholders, the Company defined the issue raised by that proposal as “requests for customer data made on the Company by government agencies.”¹³ In that no-action process and the no-action process regarding the Arjuna proposal for the 2016 annual meeting, significant policy issues at stake have variously been described as “government requests for information from telecommunications companies”¹⁴ and “consumer privacy.”¹⁵

Here, the company’s December 6, 2016 letter attempts to describe the issue raised by this proposal as “customer privacy or customer data privacy.” We object to this narrow formulation. As we have argued above, the Proposal focuses on the broad matter of *telecommunications privacy*. It queries AT&T’s position on that significant policy issue via a report on potential inconsistencies between programs like *Hemisphere* and the impressions reasonable stakeholders could form based on the Company’s own privacy policies.

The Company’s position on the broad matter of telecommunications privacy is of great interest for consumers, policymakers and the public—and, thus, a legitimate object of investor concern. Indeed, given the Company’s size and systemic importance in the telecommunications sector, that position transcends the Company’s own customers and its particular relationship with its customers. Imputing the Proposal’s subject matter to be “customer privacy or customer data privacy” would inappropriately narrow the Proposal’s concerns (perhaps to specific issues or events surrounding the Company and its own customers) and foreclose a full consideration of the widespread public debate surrounding telecommunications privacy. We encourage the Staff to resist the Company’s characterization and consider the significant policy issue of telecommunications privacy in its fullness.

¹³ <https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2014/nystatecommonatt022014-14a8.pdf>

¹⁴ *Ibid*, see p. 14

¹⁵ <https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2016/silvaweiss020516-14a8.pdf>

The Company argues that “consumer privacy” as considered in the 2016 Arjuna proposal has not — to use its word — “ripened” since the Arjuna proposal was excluded. We argue that the policy issues considered in the Arjuna proposal were defined too narrowly and do not have a bearing on this Proposal. *Telecommunications privacy* as treated in this Proposal has been a “ripened issue” for the past several years, and it has “ripened” even further since the Company excluded the Arjuna proposal in January 2016.

A. Prominence of Telecommunications Privacy as a Policy Issue

Over the years, Americans have been periodically shocked by revelations that certain of their communications are monitored, intercepted, or stored by both government and private sector actors. This has resulted in several high-profile discussions of telecommunications privacy in America, for example:

- After the revelations of NSA data collection in 2013, President Obama convened a “Review Group on Intelligence and Communications Technologies” which made several recommendations for pursuing security priorities while “Protecting the Right to Privacy.” The Review Group wrote: “The right to privacy is essential to a free and self-governing society. The rise of modern technologies makes it all the more important that democratic nations respect people’s fundamental right to privacy, which is a defining part of individual security and personal liberty.”¹⁶
- In January 2014, President Obama gave a major speech which, according to *The New York Times*, acknowledged “that high-tech surveillance poses a threat to civil liberties.” *The New York Times* reported: “Responding to the clamor over sensational disclosures about the National Security Agency’s spying practices, Mr. Obama said he would restrict the ability of intelligence agencies to gain access to phone records, and would ultimately move that data out of the hands of the government.”¹⁷
- In February 2016, Apple Inc’s refusal to circumvent encryption on an iPhone belonging to one of the perpetrators of the December 2015 San Bernardino shooting attracted major attention to the role of encryption in telecommunications privacy. *The New York Times* observed that Apple’s defenders in the ensuing dispute with the U.S. government believed that “the types of government surveillance operations exposed in 2013 by Edward J. Snowden, the former National Security Agency contractor, have prompted technology companies to build tougher encryption safeguards in their products because of the privacy demands of their customers.”¹⁸ In August 2016, FBI Director James Comey “warned again about the bureau’s inability to access digital devices because of encryption and suggested investigators wanted an ‘adult conversation’ with manufacturers.”¹⁹
- In October 2016, Yahoo came under intense criticism after revelations that it had agreed to systematically scan all of its users’ emails for specific information at the request of the FBI. The controversy threatened the company’s pending acquisition by Verizon and was

¹⁶ https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

¹⁷ <https://www.nytimes.com/2014/01/18/us/politics/obama-nsa.html? r=0>

¹⁸ <http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html>

¹⁹ <https://www.theguardian.com/technology/2016/aug/31/encryption-fbi-building-fresh-case-for-access-to-electronic-devices>

described by *The New York Times* as opening a “new chapter in a public debate over the trade-offs between security needs and privacy rights that has cast a spotlight on the sometimes cooperative, sometimes antagonistic relationship between Silicon Valley companies and the United States government.”²⁰

- Even more recently, allegations that state-sponsored actors in Russia intercepted and published communications of U.S. politicians in an attempt to influence the 2016 election have focused public attention on telecommunications privacy.²¹
- Throughout 2016, there was extensive coverage of the use of social media feeds and advanced analytics by law enforcement to surveil protesters, minorities, and suspected criminals. *The Washington Post* reported that Facebook, Twitter and Instagram “reportedly provided the data — often including the locations of users — to Geofeedia, a Chicago-based company that says it analyzes social media posts” for law enforcement agencies.²²
- In October 2016, *Ars Technica* reported that the Third Circuit Court of Appeals revived a lawsuit against the Obama administration arguing that “both the metadata and the content of his Gmail, Facebook, and Dropbox accounts were compromised under the PRISM program as revealed in the documents leaked by former National Security Agency (NSA) contractor Edward Snowden.”²³
- Throughout 2015 and 2016, there was new attention and controversy associated with law enforcement agencies’ use of “StingRay” surveillance devices. According to an April 2015 report in *The Guardian*, StingRay devices “gather information by imitating cellphone towers, scooping up metadata from all devices that connect to the fake tower.”²⁴ *FoxNews* reported in November 2016: “You may or may not have heard of a StingRay— it’s a controversial surveillance device that, by acting like a cell tower, can find your cell phone’s location and other info. Now photos of what’s reportedly a related device called a Harpoon have surfaced and show it ostensibly in the possession of the Florida Department of Law Enforcement.”²⁵
- Recent survey data suggests that events like those discussed above have made Americans concerned about telecommunications privacy. According to a 2016 Pew survey, “some 86% of internet users have taken steps online to remove or mask their digital footprints, but many say they would like to do more or are unaware of tools they could use.” Furthermore, those surveyed “express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them” while “74% say it is ‘very

²⁰ <http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html>

²¹ <http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html>

²² https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/?utm_term=.373a58167554

²³ <http://arstechnica.com/tech-policy/2016/10/appeals-court-restores-previously-dismissed-surveillance-lawsuit/>

²⁴ <https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police>

²⁵ <http://www.foxnews.com/tech/2016/11/28/florida-police-have-cell-phone-surveillance-tech-report-says.html>

important' to them that they be in control of who can get information about them, and 65% say it is 'very important' to them to control what information is collected about them."²⁶

A 2015 Pew survey found that "93% of adults say that being in control of who can get information about them is important" and "74% feel this is 'very important.'" Fully 90 percent of those surveyed said "that controlling what information is collected about them is important."²⁷

B. There is Widespread Public Debate on Telecommunications Privacy

i. General debate

In addition to being prominent in the national conversation and on the minds of ordinary Americans, telecommunications privacy is the subject of widespread and vigorous debate. Much of this debate is inspired by the events described above and a great deal of the debate specifically focuses on AT&T. The following news articles are a few representative examples of that debate:

- In December 2016 *Engadget* reported: "In a blow to privacy on par with the Patriot Act, changes to the rules around warrants grant the US government unprecedented hacking powers in any jurisdiction, and on as many devices as it wants."²⁸
- In November 2016, *The Hill* reported: "Thirty civil liberty and activist groups on Monday unveiled a to-do list for President Obama to complete before he leaves office in January, warning that President-elect Donald Trump will dangerously expand U.S. spying powers. In a letter, organizations including Demand Progress, Credo, the Electronic Frontier Foundation and FreedomWorks listed 11 areas in which the president could act before his term ends."²⁹
- In August 2016, *The Daily Dot* reported: "FBI Director James Comey, who has spent the last six months itching to get back into a public debate over the spread of encryption and mandated special backdoor government access to data, took to a spotlighted stage on Tuesday to pointedly criticize tech companies who offer default strong encryption on devices, saying he was preparing for the argument to extend into 2017 and beyond."³⁰
- In November 2016, *The New York Times* reported: "Technology, particularly rapid analysis and sharing of data, is helping the police be more efficient and predict possible crimes. Some would argue that it has even contributed to an overall drop in crime in recent years. But this type of technology also raises issues of civil liberties, as digital information provided by social media or the sensors of the internet of things is combined with criminal data by companies that sell this information to law enforcement agencies."³¹
- In November 2016, *The New York Times* reported: "The cellphone number is more than just a bunch of digits. It is increasingly used as a link to private information maintained by all

²⁶ <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

²⁷ <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>

²⁸ <https://www.engadget.com/2016/12/02/2016-claims-another-victim-your-privacy/>

²⁹ <http://thehill.com/business-a-lobbying/307062-rights-group-gives-obama-surveillance-to-do-list>

³⁰ <http://www.dailydot.com/layer8/comey-crypto-war-business-model/>

³¹ <http://www.nytimes.com/2016/11/07/technology/the-risk-to-civil-liberties-of-fighting-crime-with-big-data.html?ref=technology>

sorts of companies, including money lenders and social networks. It can be used to monitor and predict what you buy, look for online or even watch on television.”³²

- In September 2016, *The Washington Post* reported: “When a user sends someone a message through Apple’s iMessage feature, Apple encrypts that message between Apple devices so that only the sender and recipient can read its contents. But a Wednesday report from news site the Intercept is a good reminder that not all data related to iMessage has that same level of protection — and that information can still be turned over to law enforcement.”³³
- In December 2016, *NPR* reported: “A few weeks ago, Manhattan District Attorney Cyrus Vance Jr. — a vocal opponent of insurmountable encryption — renewed his call for new laws to make sure that law enforcement has a way to extract the content of locked iPhones.”³⁴
- In a November 2016 *Boston Globe* article on the FBI gaining access to the “firehose” of all tweets posted on Twitter, Kade Crockford of the American Civil Liberties Union (ACLU) said: “It’s deeply frightening that the FBI is about to access, and may already have access to, this very powerful tool.”³⁵
- In a December 2016 article in *Slate* titled “Just in Time for the Trump Administration, the FBI Has Expanded Surveillance Powers. Be afraid. Be very afraid,” Fred Kaplan wrote: “Before the new ruling, which took effect Dec. 1, a magistrate judge could issue warrants for the FBI to hack computers only within the few towns or counties of his or her jurisdiction. Now, the warrant of a single judge can allow the bureau to search online communications anywhere and everywhere in the United States, possibly even overseas.”³⁶
- In an October 2016 article titled “Privacy Debate Flares With Report About Yahoo Scanning Emails,” *The Wall Street Journal* reported: “Big technology companies, including Google, Microsoft Corp., Twitter Inc. and Facebook Inc. denied scanning incoming user emails on behalf of the U.S. government, following a report that Yahoo Inc. had built such a system.”³⁷
- In October 2016, *The Washington Post* published an article titled “Yahoo helps the government read your emails. Just following orders, they say.”
- On December 21, 2016, *Motherboard* reported on research that metadata can be used to guess an individual’s occupation. The article said: “The police line is often that you shouldn’t

³² <http://www.nytimes.com/2016/11/13/business/cellphone-number-social-security-number-10-digit-key-code-to-private-life.html?ref=technology&r=0&mtrref=undefined>

³³ https://www.washingtonpost.com/news/the-switch/wp/2016/09/30/why-apple-can-be-forced-to-turn-logs-of-your-imessage-contacts-over-to-police/?utm_term=.52ecdedd7400

³⁴ <http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>

³⁵ <https://www.bostonglobe.com/business/2016/11/24/the-fbi-just-got-access-entire-twitterverse-should-you-concerned/OPcmIvRhDneSVU1xFoXmrK/story.html>

³⁶

http://www.slate.com/articles/news_and_politics/war_stories/2016/12/a_new_ruling_gives_the_fbi_a_scary_amount_of_surveillance_power.html

³⁷ <http://www.wsj.com/articles/after-report-on-yahoo-tech-firms-deny-scanning-emails-for-u-s-government-1475627486>

worry because they're 'just' collecting metadata. But as privacy advocates and technologists have noted over and over, metadata can reveal a lot of very personal information. Now, researchers from Norwegian telecom Telenor, the MIT Media Lab, and big data nonprofit Flowminder have concluded that metadata from your cell phone can reveal if you're unemployed, or even what you do for a living."³⁸

ii. Policymakers

As a further illustration of the widespread public debate on this issue, policymakers have frequently targeted telecommunications privacy as well as AT&T's role in the issue. For example:

- In 2015, President Obama signed two major laws affecting telecommunications privacy (The USA Freedom Act and the Cybersecurity Act of 2015) which passed Congress after much heated debate.³⁹
- The FCC passed new consumer privacy rules in October 2016. According to a report in *The Washington Post*, the rules seek to limit "how Internet providers use and sell customer data, while asserting that customers have a right to control their personal information." Under the rules, "consumers may forbid Internet providers from sharing sensitive personal information, such as app and browsing histories, mobile location data and other information generated while using the Internet."⁴⁰
- In October 2016, *The New York Times* reported that the above-mentioned FCC rules frustrated the ambitions of telecommunications companies like Verizon and AT&T to build online advertising businesses.⁴¹ *CNBC* reported in October 2016 that telecommunications companies were considering suing the FCC over the new rules.⁴² On January 4, 2017, *Morning Consult* reported that industry groups were lobbying aggressively to overturn the FCC's new privacy rules at the beginning of the Trump administration.⁴³
- In response to revelations about Yahoo's email surveillance program, U.S. Representative Ted Lieu of California said "This is Big Brother on steroids and must be stopped."⁴⁴
- In December 2016, *The Wall Street Journal* reported that the U.S. House Oversight Committee "recommended Congress pass a new law to create national standards for how police officers and federal agents use powerful cellphone tracking technology in their investigations."⁴⁵

³⁸ <http://motherboard.vice.com/read/how-metadata-can-reveal-what-your-job-is>

³⁹ <http://www.msnbc.com/msnbc/senate-approves-usa-freedom-act-nsa-surveillance>;
<http://www.cnn.com/2015/12/18/politics/cybersecurity-house-senate-omnibus/>

⁴⁰ https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/?utm_term=.081a94ee7b97

⁴¹ <http://www.nytimes.com/2016/10/29/business/media/telecoms-ambitions-on-targeted-ads-seen-curbed-by-fccs-new-privacy-rules.html>

⁴² <http://www.cnn.com/2016/10/31/how-privacy-rules-will-rock-global-business-in-2017.html>

⁴³ <https://morningconsult.com/2017/01/04/industry-groups-push-overturn-fcc-privacy-rules/>

⁴⁴ https://www.washingtonpost.com/lifestyle/style/yahoo-helps-the-government-read-your-emails-just-following-orders-they-say/2016/10/05/05648894-8b01-11e6-875e-2c1bfe943b66_story.html?utm_term=.90108367a650

⁴⁵ <http://www.wsj.com/articles/house-panel-urges-new-law-for-u-s-cellphone-surveillance-1482178238>

- On December 20, *Politico* reported that the House Oversight Committee would review law enforcement agencies' use of StingRay systems. According to the report: "Stingray surveillance tech has come under fire over the past year for its ability to track cell phones, in some cases without a warrant, and even disrupt phone service for emergency calls. A new House Oversight Committee report calls for federal legislation to govern its use and make it more transparent and to provide a common standard rather than a patchwork of state policies. The report finds that DOJ and DHS spent a combined \$95 million on more than 400 stingray cell-site simulators between 2010 and 2014, and notes that grant money is set aside for state and local law enforcement to purchase the technology. On the state and local levels, the committee found the amount of court authorization needed for stingray surveillance is wildly inconsistent."⁴⁶
- In September 2016, *The Hill* reported on a lively policy debate in Congress over establishing a cellphone tracking system for missing person situations.⁴⁷

iii. Further debate over AT&T's own activity

AT&T's own experience with telecommunications privacy is also the subject of widespread debate. For example:

- The *Hemisphere* program was analyzed and debated extensively after it was first reported in 2013:
 - *ABC News*, September 2013, "DEA Program Puts Phone Company Inside Government Offices."⁴⁸
 - *CNN*, September 2013, "DEA program linked to vast AT&T database, documents show."⁴⁹
 - *The Daily Dot*, September 2013, "AT&T has a record of everywhere you've carried your phone."⁵⁰
 - *Associated Press*, September 2013, "Drug agents plumb vast database of call records."⁵¹
- In August 2015, *The Los Angeles Times* reported that the Company's conduct of its merger with DIRECTV was making it harder for customers to understand and manage their privacy. According to the article, "Instead of using the DirecTV deal as an opportunity to simplify its privacy policy, AT&T has created a more challenging process for opting out of marketing pitches from the company and its partners and for escaping AT&T's watchful gaze as you traverse the Internet."
- Beyond the news reports cited in Section II, *Hemisphere* has been analyzed and debated extensively in 2016.

⁴⁶ <http://www.politico.com/tipsheets/morning-tech/2016/12/five-potential-consequences-of-the-driverless-future-217958>

⁴⁷ <http://thehill.com/policy/technology/294659-lawmakers-wrestle-with-cellphone-tracking-for-missing-persons>

⁴⁸ <http://abcnews.go.com/blogs/headlines/2013/09/dea-program-puts-phone-company-inside-government-offices/>

⁴⁹ <http://security.blogs.cnn.com/2013/09/02/dea-program-linked-to-vast-att-database-documents-show/>

⁵⁰ <http://www.dailydot.com/layer8/att-hemisphere-nsa-dea-location-metadata/>

⁵¹ <http://www.sfexaminer.com/drug-agents-plumb-vast-database-of-call-records/>

- *Democracy Now!*, October 2016, “Project Hemisphere: AT&T's Secret Program to Spy on Americans for Profit.”⁵²
 - *The Guardian*, October 2016, “Documents show AT&T secretly sells customer data to law enforcement.”⁵³
 - *Salon*, October 2016, “AT&T helped the U.S. government spy on citizens using Project Hemisphere.”⁵⁴
 - *Breitbart*, October 2016, “Report: AT&T Being Paid by U.S. Government to Spy on Users.”⁵⁵
 - *Business Insider*, October 2016, “AT&T reportedly has a secret program that helps law enforcement spy without a warrant.”⁵⁶
 - *Newsweek*, October 2016, “AT&T spying program is ‘worse than Snowden revelations.’”⁵⁷
 - *TomDispatch*, December 2016: “Publish, Punish, and Pardon: Nine National Security Changes Obama Should Make Before He Leaves Office.”⁵⁸
- Throughout the autumn of 2016 the Company faced criticism of its proposed acquisition of Time Warner. In October 2016, *Paste Magazine* reported that *Hemisphere* and other privacy concerns could put the deal at risk.⁵⁹
 - In December 2016, *MintPress News* reported that “digital privacy and government transparency scored a victory on Thursday as a federal judge ordered the Department of Justice to provide files related to” *Hemisphere*.⁶⁰
 - In March 2015, AT&T drew criticism in the media for reported plans to sell “the privilege of not having your every click tracked, saved and regurgitated in the form of targeted ads.” According to a report in *TIME*, “the company, which just announced it’s bringing its 1-gigabit-per-second service to Kansas City, touts a price tag of \$70 per month for the high-speed connection meant to compete with services like Google Fiber. But that’s actually a “premier” offering that allows AT&T to track a user’s search terms and browsing history to serve targeted ads. The standard high-speed service without the tracking costs \$99.”⁶¹
 - AT&T’s actions surrounding *Hemisphere* and other programs have been debated by rights groups and other actors. The Company’s involvement in *Hemisphere* has been challenged in

52

<https://www.democracynow.org/2016/10/26/headlines/project-hemisphere-at-ts-secret-program-to-spy-on-americans-for-profit>

⁵³ <https://www.theguardian.com/business/2016/oct/25/att-secretly-sells-customer-data-law-enforcement-hemisphere>

⁵⁴ <http://www.salon.com/2016/10/25/att-helped-the-u-s-government-spy-on-citizens-using-project-hemisphere/>

⁵⁵ <http://www.breitbart.com/tech/2016/10/25/att-revealed-spying-users-via-secret-government-project/>

⁵⁶ <http://www.businessinsider.com/att-project-hemisphere-016-10>

⁵⁷ <http://www.newsweek.com/att-spying-program-worse-snowden-revelations-513812>

⁵⁸ <http://njtoday.net/2016/12/11/publish-punish-pardon-nine-national-security-changes-obama-make-leaves-office/>

⁵⁹ <https://www.pastemagazine.com/articles/2016/10/spying-and-big-money-deals-its-been-a-week-of-ups.html>

⁶⁰ <https://www.mintpressnews.com/judge-orders-doj-to-release-files-on-secret-spying-program-project-hemisphere/223614/>

⁶¹ <http://time.com/3713931/att-privacy-charge/>

multiple lawsuits filed by the Electronic Frontier Foundation and the Electronic Privacy Information Center.⁶² And, in October 2013, the ACLU wrote “Shocking revelations about creepy government surveillance came in waves over the summer, from the Snowden leaks to the Hemisphere Project, through which the government has paid AT&T for access to a mind-bogglingly vast database of our telephone calls. In many cases of new surveillance technologies like Hemisphere, there are serious constitutional concerns that courts have not yet reviewed.”⁶³

Telecommunications privacy and AT&T’s role in that issue are subject to continuing and vigorous debate, which has played out in the media, legislatures, regulatory forums, and civil society. The Proposal asking for a disclosure on the consistency between *Hemisphere* and the Company’s perceived approach to telecommunications privacy therefore raises a significant policy issue which is subject to widespread public debate and beyond the day-to-day affairs of the Company.

IV. The Company has not substantially implemented the Proposal and therefore is unable to exclude it pursuant to Rule 14a-8(i)(10)

The Staff has noted that a determination that a company has substantially implemented a proposal depends upon whether a company’s particular policies, practices, and procedures compare favorably with the guidelines of the proposal. *Texaco, Inc.* (Mar. 28, 1991). In the administrative history surrounding this issue, substantial implementation under Rule 14a-8(i)(10) has been variably described as satisfactorily addressing the underlying concern of the proposal, meeting the guidelines of the proposal, or meeting the essential purpose of the proposal. “Underlying concern,” which has appeared most recently, is the most lenient standard to the Company.

As stated above, the underlying concern of this Proposal is the potential inconsistency between the operation of programs like *Hemisphere* and the impressions of AT&T’s approach to telecommunications privacy invited by its policies. To satisfy that concern, the Company should disclose information about programs like *Hemisphere* in light of its existing privacy policies.

But the Company has provided virtually no information on *Hemisphere*. In the 2013 and 2016 news articles cited above, comments from the Company do not even confirm or deny the existence of the program. Indeed, the Company’s December 6, 2016 letter may constitute its first public acknowledgment of *Hemisphere*.

The Company’s Privacy Policy⁶⁴ and its most recent Transparency Report⁶⁵ mention requests from government authorities and requests associated with federal, state, and local criminal proceedings. However, those documents do not mention *Hemisphere*.

To make matters worse, the Company’s current reporting appears to obscure the existence of *Hemisphere* or similar programs in the following way. The Transparency Report publishes the number of demands for data associated with “U.S. Civil & Criminal” investigations as well as the number of those demands that were “Rejected/Challenged” or that resulted in “Partial or No

⁶² <http://epic.org/foia/dea/hemisphere/>; <https://www.eff.org/cases/hemisphere>

⁶³ <https://www.aclu.org/blog/creepy-government-surveillance-shouldnt-be-kept-secret>

⁶⁴ https://about.att.com/sites/privacy_policy

⁶⁵

https://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf

Information.” Contrary to the claim in its December 6, 2016 letter, however, AT&T *does not* disclose the number of people nor (more narrowly) the number of “customers affected” by those requests.⁶⁶

We invite the Staff to recall reports that *Hemisphere* routinely employs an extraordinarily large database and advanced, algorithmic searches to link one or more people of interest (presumably the subjects of legal demands) to many more possible associates. The current Transparency Report *does not account* for the additional possible associates because it provides only the number of demands and an indication of how many of those demands were “Rejected/Challenged.” Comparing those two figures gives an impression that the number of customers or people affected is somewhat less than the number of demands received. Thus, AT&T’s Transparency Report likely underrepresents the number of people affected by its actions with respect to U.S. Civil and Criminal Demands.

A reasonable person, even an expert, could study the Transparency Report and still fail to understand that, according to reports, AT&T’s cooperation with domestic investigations affects far more people than the number of specific legal demands. That person would walk away from the Transparency Report with no hope of understanding that, for each original person or profile of interest, *Hemisphere* routinely enables law enforcement agencies to drag many additional people into investigations. In short, the Company’s ironically-named Transparency Report hides *Hemisphere*.

Reporting which obscures the existence of *Hemisphere*, the number of people it affects, the extraordinary scope of its database, and the advanced function of its searches obviously fails to satisfy the underlying concern of this Proposal. To implement the Proposal, the company might consider, for example:

- Publicly disclosing (within the reasonable constraints discussed above) aspects of *Hemisphere* or programs like *Hemisphere*;
- Disclosing the number of people or customers affected by its actions with respect to domestic law enforcement investigations — making sure to fully consider those affected by programs like *Hemisphere*; and/or,
- Disclosing more information on potential inconsistencies between its actions regarding U.S. law enforcement investigations and stakeholders’ impressions of its approach to telecommunications privacy. This might entail a simplification or restatement (not necessarily an overhaul) of AT&T’s privacy policies, discussion of relevant examples from its experience managing the issue of telecommunications privacy, and/or publishing a study or survey on the impressions that its key outside stakeholders have formed about AT&T’s approach to telecommunications privacy.

Considering that current disclosures obscure the existence of programs like *Hemisphere* and the Company has not adopted any of the above, AT&T has failed to satisfy the Proposal’s underlying concern. It cannot hope to meet the Proposal’s guidelines or essential objective, and therefore the Proposal is not substantially implemented.

V. Conclusion

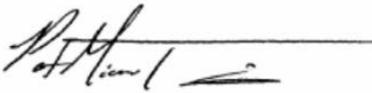
In conclusion, we respectfully request the Staff to inform the Company that Rule 14a-8 requires a denial of the Company’s no-action request.

⁶⁶ Perhaps the Company confuses its domestic (“U.S. Civil & Criminal Demands”) figures with its disclosure of “National Security Demands,” which does include “Customer Selectors Targeted.”

As demonstrated in Section II, the Proposal's requested report does not invade the Company's ordinary business operations. As demonstrated in Section III, the Proposal raises and focuses on a significant policy issue—telecommunications privacy—which has been the subject of widespread public debate. As demonstrated in Section IV, the Proposal is not substantially implemented. For these reasons, the Proposal is not excludable under Rule 14a-8.

Thank you for your consideration. In the event that the Staff should decide to concur with the Company and issue a no-action letter, we respectfully request the opportunity to speak with the Staff in advance. Please contact me at (617) 742-6666 or pat@zevin.com with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,

A handwritten signature in black ink, appearing to read "Pat Miguel Tomaino", is written over a horizontal line. The signature is cursive and somewhat stylized.

Pat Miguel Tomaino
Associate Director of Socially Responsible Investing
Zevin Asset Management, LLC



Wayne Wirtz
Vice President, Associate
General Counsel, and
Assistant Secretary

AT&T Inc.
One AT&T Plaza
208 S. Akard Street
Dallas, TX 75202

T: 214.757.3344
F: 214.746.2273
wayne.wirtz@att.com

1934 Act/Rule 14a-8

December 6, 2016

By email: shareholderproposals@sec.gov

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F St., NE
Washington, DC 20549

Re: 2017 AT&T Inc. Annual Meeting of Shareholders
Notice of Intent to Omit Shareholder Proposal of
Zevin Asset Management, LLC on behalf of
Benjamin Ewen-Campen Pursuant to Rule 14a-8

Ladies and Gentlemen:

Pursuant to Exchange Act Rule 14a-8(j), AT&T Inc., a Delaware corporation (“AT&T” or the “Company”), hereby notifies the Division of Corporation Finance of AT&T’s intention to exclude a shareholder proposal (the “2017 Proposal”) submitted by Zevin Asset Management, LLC on behalf of Benjamin Ewen-Campen (the “Proponent”) from AT&T’s proxy materials for its 2017 Annual Meeting of Shareholders (the “2017 Proxy Materials”), for the reasons stated below.

This letter, together with the 2017 Proposal and the related correspondence, are being submitted to the Staff via e-mail in lieu of mailing paper copies. A copy of this letter and the attachments are being sent on this date to the Proponent advising of AT&T’s intention to omit the 2017 Proposal from its 2017 Proxy Materials. We respectfully remind the Proponent that if he elects to submit additional correspondence to the Commission or the Staff with respect to the 2017 Proposal, a copy of that correspondence should be furnished concurrently to the undersigned pursuant to Rule 14a-8(k).

THE 2017 PROPOSAL

The 2017 Proposal, in its entirety, reads as follows:

“Whereas: There is widespread public debate about how cooperation between U.S. law enforcement entities and telecommunications companies affects Americans’ privacy and

civil rights.

Senator Edward Markey, one of many policymakers calling for regulators to review AT&T's proposed acquisition of Time Warner, remarked in October 2016: "We need a telecommunications market...where our right to privacy is maintained even when technologies change."

AT&T's Privacy Policy indicates the Company seeks to protect customer information and privacy while complying with applicable law. The July 2016 Transparency Report states: "Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements."

However, the above guidance, which indicates a cautious approach to cooperating with law enforcement agencies, is at odds with AT&T's vast Hemisphere program.

Revealing details of *Hemisphere* in 2013, *The New York Times* reported that local and federal law enforcement agencies "had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans' phone calls."

According to that report, "[t]he government pays AT&T to place [AT&T] employees in drug-fighting units around the country" and "[t]he Obama administration acknowledged the extraordinary scale of the *Hemisphere* database and the unusual embedding of AT&T employees in government drug units in three states."

In October 2016, we learned that AT&T positioned *Hemisphere* as a lucrative product aimed at a wide range of agencies and investigations. The Daily Beast reported: "Sheriff and police departments pay from \$100,000 to upward of \$1 million a year or more for Hemisphere access."

Several additional aspects of *Hemisphere* appear to go above and beyond legal requirements:

- *Hemisphere* is an extraordinarily large database going back as far as 1987, according to *The New York Times*. Other reports indicate AT&T's cellular tower data retention exceeds that of peer companies like Verizon and Sprint.
- AT&T hides *Hemisphere* by apparently requiring agencies not to use *Hemisphere* data in court unless no other evidence is available.
- *Hemisphere*'s size and AT&T's decision to offer forms of analysis which connect call records and phones to each other enable searches which would not otherwise occur.

Hemisphere and AT&T's involvement in it have prompted questions from legal experts and widespread attention from global media outlets including *The Wall Street Journal*, *Guardian*, and *Breitbart*.

While AT&T must follow the law, shareholders are concerned that failure to persuade customers of a consistent and long-term commitment to privacy rights could present serious financial, legal, and reputational risks.

Resolved: Shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on the consistency between AT&T's policies on privacy and civil rights and the Company's actions with respect to U.S. law enforcement investigations. This proposal addresses programs in use domestically like *Hemisphere*. It does not request information on international activity, national security, nor disclosures that would violate any laws."

A copy of the 2017 Proposal and related correspondence with the Proponent is attached to this letter as Exhibit A.

ARGUMENT

The Company believes that the 2017 Proposal may be properly excluded from the 2017 Proxy Materials pursuant to:

- Rule 14a-8(i)(7), because the 2017 Proposal deals with a matter relating to the Company's ordinary business operations; and
- Rule 14a-8(i)(10), because the 2017 Proposal has been substantially implemented by the Company, which has addressed the subject matter of the 2017 Proposal in existing reports and public disclosures.

A. The 2017 Proposal Relates to Ordinary Business Matters and Therefore May Be Excluded From the 2017 Proxy Materials Pursuant to Rule 14a-8(i)(7).

Rule 14a-8(i)(7) permits a company to omit a shareholder proposal from its proxy materials if the proposal deals with a matter relating to the company's "ordinary business operations." The purpose of the ordinary business exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting."¹ Two considerations underlie this exclusion. The first relates to the subject matter of the proposal: "[c]ertain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight."² The second consideration relates to the "degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not

¹ Release No. 34-40018 (May 21, 1998) (the "1998 Release").

² *Id.*

be in a position to make an informed judgment.”³

In applying Rule 14a-8(i)(7) to proposals requesting companies to prepare reports on specific aspects of their business, the Staff has determined that it will consider whether the subject matter of the report involves a matter of ordinary business. If it does, the proposal can be excluded even if it requests only the preparation of the report and not the taking of any action with respect to such ordinary business matter.⁴

Protection of Customer Privacy is an Ordinary Business Matter

The 2017 Proposal can be excluded under Rule 14a-8(i)(7) because it focuses on the Company’s policies for protecting customer privacy in the context of governmental requests for customer information. The Staff has repeatedly recognized that the protection of customer privacy is a core management function not subject to shareholder oversight, and the Staff has done so specifically with regard to AT&T. In fact, just last year the Staff concurred in the Company’s exclusion of a similar proposal (the “2016 Proposal”) requesting that the Company issue a report “clarifying the Company’s policies regarding providing information to law enforcement and intelligence agencies.”⁵ There, the Staff issued a no-action letter stating it would not object if the Company excluded the proposal on the ground that it “relates to procedures for protecting customer information and does not focus on a significant policy issue.” In addition, in connection with its annual meetings in 2007 and 2009, the Company received proposals similar to the 2016 and 2017 Proposals, and in each case the Staff issued a no-action letter confirming it would not recommend any enforcement action if the Company excluded the proposal from its annual proxy materials because the proposal related to the Company’s ordinary business operations.⁶

The 2017 Proposal bears a striking resemblance to the excluded 2016 Proposal. For convenience, the “Resolved” clause of each of the 2016 Proposal and 2017 Proposal are provided below:

2016 Proposal

“Resolved, shareholders request that the Company issue a report, at reasonable expense and excluding proprietary or legally protected information, clarifying the Company’s

³ *Id.*

⁴ Release No. 34-20091 (Aug. 16, 1983).

⁵ *AT&T Inc.* (Feb. 5, 2016)

⁶ The 2007 meeting proposal also requested the preparation of a report regarding disclosure of customer communications and related information to specified governmental agencies without a warrant. *AT&T Inc.* (Feb. 9, 2007). The 2009 meeting proposal requested the preparation of a report addressing privacy and free expression in the context of internet providers; the Staff permitted it to be excluded on the ground that “it related to AT&T’s ordinary business operations (i.e., procedures for protecting user information).” *AT&T Inc.* (January 26, 2009).

policies regarding providing information to law enforcement and intelligence agencies, domestically and internationally, above and beyond what is legally required by court order or other legally mandated process, whether and how the policies have changed since 2013, and assessing risks to the Company's finances and operations arising from current and past policies and practices." (Emphasis added.)

2017 Proposal

"Resolved: Shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on the consistency between AT&T's policies on privacy and civil rights and the Company's actions with respect to U.S. law enforcement investigations. This proposal addresses programs in use domestically like *Hemisphere*. It does not request information on international activity, national security, nor disclosures that would violate any laws." (Emphasis added.)

Therefore, as demonstrated by its "Resolved" clause, the 2017 Proposal is effectively a repackaging of the excluded 2016 Proposal. While the 2017 Proposal differs from the excluded 2016 Proposal by (1) concentrating only on law enforcement agencies versus law enforcement and intelligence agencies and (2) focusing only on domestic programs, such as *Hemisphere*, versus domestic and international programs, both proposals would require the Company to subject its customer privacy policies to the oversight of shareholders at an annual meeting. As such, the 2017 Proposal may also properly be excluded pursuant to Rule 14a-8(i)(7).

In addition, the Staff has granted no-action relief to other major telecommunications companies in response to shareholder proposals relating to customer privacy and the provision of customer records and communications content to governmental authorities.⁷ The Staff has also recognized customer privacy as an ordinary business matter for companies outside the telecommunications industry.⁸

The 2017 Proposal Relates to Matters of Legal Compliance

The 2017 Proposal may also be properly excluded pursuant to Rule 14a-8(i)(7) because it implicates the Company's conduct of its legal compliance program. The Staff has long viewed a company's compliance with laws and regulations as a matter of ordinary business. The Staff recently permitted Navient Corporation to exclude a proposal calling for a report on its internal controls over its student loan servicing

⁷ See, e.g., *Sprint Nextel Corporation* (Feb. 17, 2009); *Verizon Communications Inc.* (Feb. 22, 2007).

⁸ See, e.g., *Applied Digital Solutions, Inc.* (Mar. 25, 2006) (proposal requesting the company to prepare a report analyzing the privacy implications of its radio frequency identification chips could be excluded as relating to ordinary business matters); *Bank of America Corp.* (Feb. 21, 2006) (proposal requesting a report on company policies and procedures for ensuring the confidentiality of customer information could be excluded as relating to ordinary business matters).

operations, including a discussion of the actions taken to ensure compliance with applicable law.⁹ In permitting this exclusion, the Staff stated that “[p]roposals that concern a company’s legal compliance program are generally excludable under Rule 14a-8(i)(7).” Much like the 2016 Proposal, the 2017 Proposal plainly seeks review and oversight of the Company’s legal compliance program relating to the provision of information to law enforcement; it is impossible to dissociate the information sought by the 2017 Proposal from the Company’s legal compliance program relating to the provision of information to governmental agencies.

The 2017 Proposal Does Not Focus on a Significant Policy Issue.

The Commission has stated that “proposals relating to such [ordinary business] matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable because the proposals would transcend the day-to-day business matter and raise policy matters so significant that it would be appropriate for a shareholder vote.”¹⁰ In determining matters that rise to the level of a “significant policy issue” for purposes of Rule 14a-8, the Staff has focused on whether the issue has been the focus of sustained and growing public debate.¹¹

In the no-action correspondence regarding the Company’s request to exclude the 2016 Proposal from its 2016 annual meeting proxy materials, the proponent of the 2016 Proposal argued that consumer privacy was a “ripened issue” and that the “accumulated evidence *today* documents that this issue has attained the high profile issue meeting all of the Staff’s criteria for a significant policy issue”¹² (emphasis in original). The 2016 proponent also requested information concerning cooperation with law enforcement, including through the *Hemisphere* program referenced in the 2017 Proposal, in addition to other information regarding cooperation with intelligence gathering agencies.

The Staff concluded that the subject of the 2016 Proposal, including information regarding cooperation with domestic law enforcement, was a matter of ordinary business

⁹ *Navient Corp.* (Mar. 26, 2015). See also, e.g., *FedEx Corp.* (Jul. 14, 2009), *Verizon Communications Inc.* (Jan. 7, 2008), *The AES Corporation* (Jan. 9, 2007), *Halliburton Company* (Mar. 10, 2006), *Allstate Corp.* (Feb. 16, 1999), *Duke Power co.* (Feb. 1, 1988).

¹⁰ 1998 Release.

¹¹ See, e.g., *Philip Morris Cos. Inc.* (Feb. 22, 1990) (not permitting exclusion of a proposal requesting a “Review Committee” to analyze the impact of the company’s tobacco advertising on minors because of the “growing significance of the social and public policy issues attendant to operations involving the manufacture and distribution of tobacco related products”) (emphasis added).

¹² See January 5, 2016 letter from Natasha Lamb, Director of Equity Research & Shareholder Engagement, Arjuna Capital, available at: <https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2016/silvaweiss020516-14a8.pdf>.

operations.¹³ There is no reason for the Staff to change its view today. The level of public debate about customer privacy or customer data privacy has not meaningfully changed since January 2016. The Company, therefore, believes that it may properly exclude the 2017 Proposal from its 2017 Proxy Materials in reliance on Rule 14a-8(i)(7).

B. The 2017 Proposal Has Been Substantially Implemented and May Be Excluded Pursuant to Rule 14a-8(i)(10).

Rule 14a-8(i)(10) provides that a company may exclude a proposal from its proxy materials if “the company has already substantially implemented the proposal.” According to the Commission, this exclusion “is designed to avoid the possibility of shareholders having to consider matters which have already been favorably acted upon by management.”¹⁴ The Staff has articulated this standard by stating that “a determination that the company has substantially implemented the proposal depends upon whether particular policies, practices and procedures compare favorably with the guidelines of the proposal.”¹⁵ A company need not implement every detail of a proposal in order for the Staff to permit exclusion under Rule 14a-8(i)(10).¹⁶ Rather, the Staff has consistently permitted exclusion of a shareholder proposal when a company already has policies and procedures in place satisfactorily addressing the underlying concerns of the proposal or has implemented the essential objectives of the proposal.¹⁷

¹³ *AT&T, Inc.* (Feb. 5, 2016).

¹⁴ See Release No. 34-20091 (Aug. 16, 1983) (the “1983 Release”).

¹⁵ *Texaco, Inc.* (Mar. 28, 1991) (proposal requesting the company to implement a specific set of environmental guidelines was excluded as substantially implemented because the company had established a compliance and disclosure program related to its environmental program, even though the company’s guidelines did not satisfy the specific inspection, public disclosure or substantive commitments that the proposal sought).

¹⁶ See 1983 Release.

¹⁷ See, e.g., *Dominion Resources, Inc.* (Feb. 9, 2016) (proposal requesting the company to publish a report on measuring, mitigating, disclosing and setting reduction targets for methane emissions was excludable where existing company disclosures compared favorably to the guidelines of the proposal, in spite of the proponent’s allegation that the company’s disclosures did not cover all facilities, address means of measuring methane reduction, or include specific reduction targets); *Pfizer Inc.* (Jan. 11, 2013) (proposal requesting the company to produce a report on measures implemented to reduce the use of animal testing and plans to promote alternatives to animal use was excludable where existing company laboratory animal care guidelines and policy were available on its website); *MGM Resorts International* (Feb. 28, 2012) (proposal requesting a report on the company’s sustainability policies and performance, including multiple, objective statistical indicators, permitted to be excluded where the company published an annual sustainability report); *Duke Energy Corp.* (Feb. 21, 2012) (proposal requesting that an independent board committee assess and prepare a report on the company’s actions to build shareholder value and reduce greenhouse gas and other emissions was permitted to be excluded in light of the company’s existing policies, practices and procedures and public disclosures); *ConAgra Foods, Inc.* (July 3, 2006) (proposal requesting a sustainability report was permitted to be excluded where the company already published a sustainability report as part of its corporate responsibilities report); and *The Talbots Inc.* (Apr. 5, 2002) (proposal requesting the company letter to implement a code of conduct based on International Labor Organization human rights standard was permitted to be excluded in light of the company’s own business

As noted above, the 2017 Proposal focuses on information about the Company's policies and actions regarding the provision of customer information to law enforcement agencies. However, the Company already produces Transparency Reports on this very topic on a semiannual basis. These reports provide detailed data concerning the number of law enforcement and intelligence agency demands the Company receives and the Company's responses to those demands, as well as a description of its policies and practices.¹⁸ Each Transparency Report contains, to the extent permitted by law:

- the total number of U.S. Criminal and Civil Demands received, including, pursuant to subpoenas, court orders and warrants, and the number of customers affected;
- the total number of National Securities Letters and Foreign Intelligence Surveillance Act orders received and the number of customer accounts affected;
- the total number of emergency requests received; and
- the total number of international demands received.

In addition, the Transparency Reports contain descriptions of the Company's practices and procedures for responding to various types of demands for information from law enforcement and intelligence agencies. These can be found, for example, on pages 6 through 10 of the Transparency Report that AT&T published for the first six-month period in 2016.¹⁹ AT&T has also adopted a Privacy Policy, appointed a Chief Privacy Officer and trained relevant employees on compliance with the Privacy Policy.²⁰ The Privacy Policy describes the Company's practices and procedures for protecting the confidentiality of customer information and how the Company implements and updates them. The Company posts publicly on its website prominent notices of important pending changes to the Privacy Policy at least 30 days before the effective date.²¹

The Company's Transparency Reports and Privacy Policy substantially implement and compare favorably to the report requested in the 2017 Proposal. Like the 2017 Proposal, both the Transparency Report and the Privacy Policy focus on the Company's policies regarding the provision of customer information to law enforcement agencies, and the 2017 Proposal may therefore be excluded pursuant to Rule 14a-8(i)(10).

practice standards).

¹⁸ The Transparency Reports are available at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>.

¹⁹ AT&T July 2016 Transparency Report, available at: http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf.

²⁰ The Company's Privacy Policy is available at <http://www.att.com/gen/privacy-policy?pid=2506>.

²¹ *Id.*

CONCLUSION

Based on the foregoing analysis, we respectfully request the Staff concur that it will take no action if Company excludes the 2017 Proposal from its 2017 Proxy Materials in reliance on Rule 14a-8. We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to me at ww0118@att.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (214) 757-3344.

Sincerely,

A handwritten signature in black ink that reads "Wayne Wirtz". The signature is written in a cursive style and is contained within a light gray rectangular box.

Wayne Wirtz

Exhibit A: Proposal

cc: Pat Miguel Tomaino, Zevin Asset Management, LLC

Zevin Asset Management, LLC

PIONEERS IN SOCIALLY RESPONSIBLE INVESTING

November 10, 2016

VIA OVERNIGHT MAIL & E-MAIL

Stacey Maris
Senior Vice President and Secretary
AT&T, Inc.
208 S. Akard Street
Suite 3241
Dallas, Texas 75202

Re: Shareholder Proposal for 2017 Annual Meeting

Dear Ms. Maris:

Enclosed please find our letter filing the proposal on privacy to be included in the proxy statement of AT&T, Inc. ("AT&T" or the "Company") for its 2017 annual meeting of stockholders.

Zevin Asset Management is a socially responsible investment manager which integrates financial and environmental, social, and governance research in making investment decisions on behalf of our clients. We are concerned about the apparent inconsistency between AT&T's privacy policies and its actions with respect to U.S. law enforcement investigations. Therefore, we are filing this proposal asking for a report reviewing potential inconsistencies.

We are filing on behalf of one of our clients, Benjamin Ewen-Campen (the Proponent), who has continuously held, for at least one year of the date hereof, 1900 shares of the Company's stock which would meet the requirements of Rule 14a-8 under the Securities Exchange Act of 1934, as amended. Verification of this ownership from a DTC participating bank (number 0221), UBS Financial Services Inc, is enclosed.

Zevin Asset Management, LLC has complete discretion over the Proponent's shareholding account at UBS Financial Services Inc which means that we have complete discretion to buy or sell investments in the Proponent's portfolio. Let this letter serve as a confirmation that the Proponent intends to continue to hold the requisite number of shares through the date of the Company's 2017 annual meeting of stockholders.

Zevin Asset Management, LLC is the lead filer for this proposal. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

Zevin Asset Management welcomes the opportunity to discuss the proposal with representatives of the Company. Please forward any correspondence relating to this matter to Zevin Asset Management. Please confirm receipt of this proposal to me at 617-742-6666 or via email at pat@zevin.com.

Sincerely,



Pat Miguel Tomaino
Associate Director of Socially Responsible Investing
Zevin Asset Management, LLC

Whereas: There is widespread public debate about how cooperation between U.S. law enforcement entities and telecommunications companies affects Americans' privacy and civil rights.

Senator Edward Markey, one of many policymakers calling for regulators to review AT&T's proposed acquisition of Time Warner, remarked in October 2016: "We need a telecommunications market...where our right to privacy is maintained even when technologies change."

AT&T's Privacy Policy indicates the Company seeks to protect customer information and privacy while complying with applicable law. The July 2016 Transparency Report states: "Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements."

However, the above guidance, which indicates a cautious approach to cooperating with law enforcement agencies, is at odds with AT&T's vast *Hemisphere* program.

Revealing details of *Hemisphere* in 2013, *The New York Times* reported that local and federal law enforcement agencies "had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans' phone calls."

According to that report, "[t]he government pays AT&T to place [AT&T] employees in drug-fighting units around the country" and "[t]he Obama administration acknowledged the extraordinary scale of the *Hemisphere* database and the unusual embedding of AT&T employees in government drug units in three states."

In October 2016, we learned that AT&T positioned *Hemisphere* as a lucrative product aimed at a wide range of agencies and investigations. *The Daily Beast* reported: "Sheriff and police departments pay from \$100,000 to upward of \$1 million a year or more for *Hemisphere* access."

Several additional aspects of *Hemisphere* appear to go above and beyond legal requirements:

- *Hemisphere* is an extraordinarily large database going back as far as 1987, according to *The New York Times*. Other reports indicate AT&T's cellular tower data retention exceeds that of peer companies like Verizon and Sprint.
- AT&T hides *Hemisphere* by apparently requiring agencies not to use *Hemisphere* data in court unless no other evidence is available.
- *Hemisphere*'s size and AT&T's decision to offer forms of analysis which connect call records and phones to each other enable searches which would not otherwise occur.

Hemisphere and AT&T's involvement in it have prompted questions from legal experts and widespread attention from global media outlets including *The Wall Street Journal*, *Guardian*, and *Breitbart*.

While AT&T must follow the law, shareholders are concerned that failure to persuade customers of a consistent and long-term commitment to privacy rights could present serious financial, legal, and reputational risks.

Resolved: Shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on the consistency between AT&T's policies on privacy and civil rights and the Company's actions with respect to U.S. law enforcement investigations. This proposal addresses programs in use domestically like *Hemisphere*. It does not request information on international activity, national security, nor disclosures that would violate any laws.

Zevin Asset Management, LLC

PIONEERS IN SOCIALLY RESPONSIBLE INVESTING

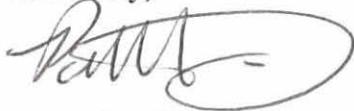
November 10, 2016

To Whom It May Concern:

Please find attached UBS Financial Services custodial proof of ownership statement of AT&T Inc (T) from Benjamin Ewen-Campen. Zevin Asset Management, LLC is the investment advisor to Benjamin Ewen-Campen and filed a shareholder resolution on privacy on Benjamin Ewen-Campen's behalf.

This letter serves as confirmation that Benjamin Ewen-Campen is the beneficial owner of the above referenced stock.

Sincerely,



Pat Miguel Tomaino
Associate Director of Socially Responsible Investing
Zevin Asset Management, LLC



UBS Financial Services Inc.
One Post Office Square
Boston, MA 02109
Tel. 617-439-8000
Fax 617-439-8474
Toll Free 800-225-2385

www.ubs.com

November 10, 2016

To Whom It May Concern:

This is to confirm that DTC participant (number 0221) UBS Financial Services Inc is the custodian for 1,900 shares of common stock in AT&T (T) owned by Benjamin Ewen-Campen.

We confirm that the above account has beneficial ownership of at least \$2,000 in market value of the voting securities of AT&T and that such beneficial ownership has continuously existed for one or more years in accordance with rule 14a-8(a)(1) of the Securities Exchange Act of 1934.

The shares are held at Depository Trust Company under the Nominee name of UBS Financial Services.

This letter serves as confirmation that Benjamin Ewen-Campen is the beneficial owner of the above referenced stock.

Zevin Asset Management, LLC is the investment advisor to Benjamin Ewen-Campen and is planning to co-file a shareholder resolution on behalf of Benjamin Ewen-Campen.

Sincerely,

A handwritten signature in black ink, appearing to read "Kelley A. Bowker".

Kelley A. Bowker
Assistant to Myra G. Kolton
Senior Vice President Wealth Management