



DIVISION OF  
CORPORATION FINANCE

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

February 5, 2016

Wayne A. Wirtz  
AT&T Inc.  
ww0118@att.com

Re: AT&T Inc.  
Incoming letter dated December 7, 2015

Dear Mr. Wirtz:

This is in response to your letters dated December 7, 2015, January 14, 2016 and January 29, 2016 concerning the shareholder proposal submitted to AT&T by Arjuna Capital on behalf of John Silva and Shana Weiss. We also have received letters on the proponents' behalf dated January 5, 2016, January 27, 2016 and February 4, 2016. 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: Natasha Lamb  
Arjuna Capital/Baldwin Brothers Inc.  
natasha@arjuna-capital.com

February 5, 2016

**Response of the Office of Chief Counsel**  
**Division of Corporation Finance**

Re: AT&T Inc.  
Incoming letter dated December 7, 2015

The proposal requests that the company issue a report clarifying its 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 those policies have changed since 2013, and assessing risks to the company's finances and operations arising from current and past policies and practices.

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 and does not focus on a significant policy issue. 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 bases for omission upon which AT&T relies.

Sincerely,

Ryan J. Adams  
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 matter 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 proposals 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 administered by the Commission, including argument as to whether or not activities proposed to be taken would be violative of 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 adversary procedure.

It is important to note that the staff's and Commission'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 shareholders 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 management omit the proposal from the company's proxy material.

February 4, 2016

VIA e-mail: [shareholderproposals@sec.gov](mailto:shareholderproposals@sec.gov)

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

Re: AT&T Inc.'s January 29, 2016 second Supplemental No Action Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss  
Securities and Exchange Act of 1934—Rule 14a-8

Dear Sir/Madam:

This letter is submitted on behalf of John Silva and Shana Weiss, as their designated representative in this matter, and (hereinafter referred to as the “Proponents”), who are beneficial owners of shares of common stock of AT&T Incorporated (hereinafter referred to as “AT&T” or the “Company”), and who have submitted a shareholder proposal (hereinafter referred to as “the Proposal”) to AT&T, to respond to the supplemental letter dated January 29<sup>th</sup>, 2016 sent to the Office of Chief Counsel by the Company, in which AT&T contends that the Proposal may be excluded from the Company's 2016 proxy statement under Rule 14a-8:

- Rule 14a-8(i)(2), because implementation of the Proposal by the Company would violate Federal law;
- Rule 14a-8(i)(7), because the Proposal deals with a matter relating to the Company's ordinary business operations; and
- Rule 14a-8(i)(10), because the Proposal has been substantially implemented by the Company, which has addressed the subject matter of the Proposal in existing reports and public disclosures.

We have further reviewed the Company's second supplemental letter and the contents of the Proposal, and it is our opinion that the Proposal should be included in AT&T's 2016 proxy statement because shareholders require a legal, transparent understanding of how AT&T is protecting the privacy of its customers.

The Company continues to conflate the Proponent's request for a discussion of the Company's policies and practices with the disclosure of classified information, notwithstanding our repeated disclaimers that we do not seek confidential information and that our request specifically excludes “proprietary or legally protected information.”

The Company cites the opinion of its own outside legal counsel as a definitive analysis as to whether the Company could implement the Proposal were it so inclined, further asserting that Proponent's arguments are “merely a statement by the Director of Equity Research & Shareholder Engagement at Arjuna Capital.” We note that Sidley, according to its web site, has represented AT&T Inc. and its predecessors “for more than a century.” The Proponent's arguments are respectful, straightforward and well-reasoned – representing the legitimate interests of the Company's shareholders.

As for the Company's argument regarding ordinary business, we note that the Company's semi-annual Transparency Reports concerning government requests for data do not disclose or discuss the Company's cooperation “above and beyond what is legally required by court order or other legally mandated process,” as requested in the Proposal.

In light of the extensive information requested in the Proposal that is not fulfilled by the Company's existing reporting and the clear mandate to disclose at a policy level, the Company has not acted favorably on the contents of this proposal. We therefore call on the Company to clarify its role in providing information to

government entities above and beyond its legal duty. 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 are providing a copy to AT&T's Associate General Counsel Wayne Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com).

Please contact me at (978) 578-4123 or [natasha@arjuna-capital.com](mailto:natasha@arjuna-capital.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 'NL', with a long horizontal flourish extending to the right.

Natasha Lamb  
Director of Equity Research & Shareholder Engagement  
Arjuna Capital

cc: Wayne A. Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com)  
Associate General Counsel  
AT&T Incorporated



Wayne A. Wirtz  
Associate General Counsel  
Legal Department  
208 S. Akard, Room 3024  
Dallas, Texas 75202  
(214) 757-3344  
ww0118@att.com  
1934 Act/Rule 14a-8

January 29, 2016

***By email: [shareholderproposals@sec.gov](mailto: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: 2016 AT&T Inc. Annual Meeting of Shareholders – 2d Supplemental Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss Pursuant to Rule 14a-8

Ladies and Gentlemen:

This supplemental letter is submitted in response to correspondence from Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss (collectively, the “Proponent”) dated January 28, 2016, in connection with the above-referenced proposal (the “Proposal”). This letter, which will be brief, should be read in conjunction with AT&T’s December 7, 2015, initial submission and its later correspondence dated January 14, 2016.

\* \* \*

The Proposal requests that the Company:

“...issue a report, at reasonable expense and excluding proprietary or legally protected information, clarifying the Company’s 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.”

In its submissions in response to the Proposal, AT&T has met its burden to show that the Proposal may properly be omitted from the 2016 Proxy Materials on several grounds, including the ground that implementation of the Proposal would cause the Company to violate Federal law. On this point, AT&T has provided a legal opinion from the law firm of Sidley Austin LLP, which states:

“...we are of the opinion that AT&T would violate the Referenced Federal Statutes [18 U.S.C. §798(a) and Section 6 of the National Security Agency Act] if it were to implement the Proposal.”

The Proponent, on the other hand, has not provided any legal opinion or legal analysis refuting the Sidley opinion. Instead, the Proponent simply states in its January 28 response that: “it is our opinion that the Proposal should be included in AT&T’s 2016 proxy statement because shareholders require a legal, transparent understanding of how AT&T is protecting the privacy of its customers.” This is not a legal opinion or analysis, and it does not refute the Sidley opinion. It is merely a statement by the Director of Equity Research & Shareholder Engagement at Arjuna Capital, advocating for a policy that the law does not permit.<sup>1</sup> Therefore, the Proposal may be properly omitted pursuant to Rule 14a-8(i)(2).

In addition, even though the Proponent now seeks to distance itself from the national security implications of its Proposal – despite the clear language of the Proposal – it remains that the Proposal may also be properly omitted under Rules 14a-8(i)(7) and (10). With respect to Rule 14a-8(i)(7), regardless of whether we accept the Proponent’s claim in the January 28 response that the Proposal excludes legally protected information, the Proposal would still relate to matters of legal compliance and customer privacy, each of which is a matter of ordinary business. With respect to Rule 14a-8(i)(10), the Company has substantially implemented the Proposal through existing policies, procedures and reports, including the semi-annual Transparency Reports, which provide, to the extent permitted by law, detailed data concerning the number of law enforcement and intelligence agency demands that the Company receives as well as the Company’s responses to those demands.

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](mailto: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,

  
Wayne Wirtz

cc: Natasha Lamb, Arjuna Capital

---

<sup>1</sup> In addition, Proponent continues to willfully mischaracterize the facts regarding AT&T’s Transparency Reports. In its January 28 response, Proponent falsely reports that AT&T stated in December 2013 that it would provide classified information about governmental requests. In fact, at that time, AT&T only stated it would provide information about *law enforcement requests*; it made no reference to disclosing classified information. It was only *after* the Director of National Intelligence in January 2014 de-classified certain specified aggregate data concerning requests for customer information that AT&T decided to expand its Transparency Report to include the de-classified information. The first Transparency Report was subsequently issued on February 17, 2014.

January 27, 2016

VIA e-mail: [shareholderproposals@sec.gov](mailto:shareholderproposals@sec.gov)

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

Re: AT&T Inc.'s January 14, 2016 Supplemental No Action Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss  
Securities and Exchange Act of 1934—Rule 14a-8

Dear Sir/Madam:

This letter is submitted on behalf of John Silva and Shana Weiss, as their designated representative in this matter, and (hereinafter referred to as the “Proponents”), who are beneficial owners of shares of common stock of AT&T Incorporated (hereinafter referred to as “AT&T” or the “Company”), and who have submitted a shareholder proposal (hereinafter referred to as “the Proposal”) to AT&T, to respond to the supplemental letter dated January 14<sup>th</sup>, 2016 sent to the Office of Chief Counsel by the Company, in which AT&T contends that the Proposal may be excluded from the Company's 2016 proxy statement under Rule 14a-8:

- Rule 14a-8(i)(2), because implementation of the Proposal by the Company would violate Federal law;
- Rule 14a-8(i)(7), because the Proposal deals with a matter relating to the Company's ordinary business operations; and
- Rule 14a-8(i)(10), because the Proposal has been substantially implemented by the Company, which has addressed the subject matter of the Proposal in existing reports and public disclosures.

We have further reviewed the Company's supplemental letter and the contents of the Proposal, and it is our opinion that the Proposal should be included in AT&T's 2016 proxy statement because shareholders require a legal, transparent understanding of how AT&T is protecting the privacy of its customers.

The Company's latest reply, accompanied by the Sidley opinion, contains a considerable volume of language. The Proponent's reply is straightforward.

The Company previously argued to the Staff, in December 2013, that “any information about assistance that AT&T has, or has not, provided to the government in connection with the government's foreign intelligence surveillance activities would almost certainly be classified information that AT&T could not legally disclose.” Yet two weeks after making that statement, and following a similar announcement by its competitor Verizon Communications, the Company publicly agreed to publish semi-annual transparency reports, providing considerable detail within legal constraints.

As the Company notes in its most recent reply, the U.S. government declassified certain information *one month later, subsequent* to the Company's already announced agreement to publish transparency reports.

We find ourselves now in a similar situation, as the Company asserts once again that it cannot legally discuss *any information* about assistance that AT&T has or has not provided to intelligence agencies. As we have argued, Proponents are not requesting disclosure of classified information but, rather, discussion of the Company's policies in this regard.

Specifically, the proposal asks:

The Company issue a report, at reasonable expense and **excluding proprietary or legally protected information, clarifying the Company's 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. [Proponent's emphasis]

Our request is not asking the Company to disclose information that would violate federal law. To the contrary, we *explicitly* ask the Company to *exclude* legally protected information. Instead, we are asking for greater understanding of how the Company is managing the "financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy 'to the fullest extent possible.'"

We are disturbed by the Company's previous assertion that the "protection of customer privacy is an ordinary business concern" in the wake of such intense public controversy over breaches of AT&T's customers' civil liberties. As we noted in our prior response, the level of engagement by media, legislators, President Obama, other heads of state, and the public on these issues of trust and transparency is exemplary of a significant social policy issue.

The Proposal is explicit in its request to clarify "the Company's policies regarding providing information to **law enforcement** and intelligence agencies, domestically and internationally..." which appears squarely in the Resolved Clause [Proponent's emphasis]. The Company's argues that information related to law enforcement activities that is not legally protected, is ordinary business. The Proponents draw no distinction between issues of grave concern to the civil liberties of our citizens and AT&T's customers in a law enforcement or intelligence gathering context. We seek a clarification on how relationships with both forms of entities are managed at the policy level.

In light of the extensive information requested in the Proposal that is not fulfilled by the Company's existing reporting and the clear mandate to disclose at a policy level, the Company has not acted favorably on the contents of this proposal. We therefore call on the Company to clarify its role in providing information to government entities above and beyond its legal duty. 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 are providing a copy to AT&T's Associate General Counsel Wayne Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com).

Please contact me at (978) 578-4123 or [natasha@arjuna-capital.com](mailto:natasha@arjuna-capital.com) with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Natasha Lamb  
Director of Equity Research & Shareholder Engagement  
Arjuna Capital

cc: Wayne A. Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com)  
Associate General Counsel  
AT&T Incorporated



Wayne A. Wirtz  
Associate General Counsel  
Legal Department  
208 S. Akard, Room 3024  
Dallas, Texas 75202  
(214) 757-3344  
ww0118@att.com

1934 Act/Rule 14a-8

January 14, 2016

***By email: [shareholderproposals@sec.gov](mailto: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: 2016 AT&T Inc. Annual Meeting of Shareholders – Supplemental Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss Pursuant to Rule 14a-8

Ladies and Gentlemen:

Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss (collectively, the “Proponent”) submitted a shareholder proposal and statement in support thereof (collectively, the “Proposal”) to AT&T Inc. (“AT&T” or the “Company”) for inclusion in AT&T’s proxy statement and form of proxy for its 2016 Annual Meeting of Shareholders (collectively, the “2016 Proxy Materials”). The Proposal requests that the Company “issue a report, at reasonable expense and excluding proprietary or legally protected information, clarifying the Company’s 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.”

This supplemental letter is submitted in response to a letter from the Proponent, dated January 5, 2016 (the “January 5 Response”), and should be read in conjunction with AT&T’s December 7, 2015 letter to the Staff, notifying it of AT&T’s intent to exclude the Proposal pursuant to Exchange Act Rule 14a-8 (the “December 7 Submission”).

## ARGUMENT

### ***The January 5 Response Supports the Conclusion that the Proposal May Be Omitted Because Its Implementation Would Violate Federal Law.***

First and most importantly, the January 5 Response fails to address in any meaningful way the Company's argument that implementing the Proposal would cause the Company to violate federal law.

The January 5 Response leaves no doubt that the Proposal is centrally and directly aimed at requesting AT&T to disclose the full extent of any relationship it may have with the National Security Agency ("NSA"). The January 5 Response characterizes the Proposal as follows: "The Proponents do not seek classified information, but a clear understanding of the Company's role in a controversy that spans nearly 15 years. Specifically, the proposal asks AT&T to clarify their policy of providing information to domestic and international law enforcement and intelligence agencies above and beyond what is legally required by court order or other legally mandated process."

As stated in the legal opinion from Sidley Austin LLP, provided with and incorporated into the December 7 Submission, the Company cannot implement the Proposal in good faith without, at a minimum, either confirming or denying whether it provides information to the NSA "above and beyond what is legally required by court order or other legally mandated process." In Sidley's opinion, this is the very type of information the Company cannot disclose without violating the law – specifically, 18 U.S.C. § 798(a) and 50 U.S.C. § 402 note – because such information would be subject to "any legal provision that would otherwise prohibit the disclosure of classified data, including data relating to FISA surveillance."<sup>1</sup>

The January 5 Response (i) ignores the substance of this reasoned legal opinion; (ii) provides misleading assertions to support its conclusory statement that the December 7 Submission is "obviously incorrect"; and (iii) otherwise offers no analysis, legal or otherwise, contradicting Sidley's opinion. Specifically, the January 5 Response misleadingly asserts that Sidley's opinion and AT&T's analysis and conclusions contained in the December 7 Submission are "contradicted by the Company's own actions regarding Proponent's 2014 proposal," which requested "that the Company publish semi-annual reports, subject to existing laws and regulation, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information."<sup>2</sup> The Company's "own actions" – namely, its decision to begin issuing transparency reports in early 2014 – are characterized by the January 5 Response as follows: "Yet, only two weeks later, the

---

<sup>1</sup> Notice to the U.S. Foreign Intelligence Surveillance Court by the United States, *In re Amended Motion for Decl. Judgment*, Jan. 27, 2014, available at <http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf>.

<sup>2</sup> See AT&T's December 5, 2013 submission to the Staff, available at <http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2014/nystatecommonatt022014-14a8.pdf>.

Company announced that it would publish regular reports concerning government requests for confidential customer information.”

This statement is misleading. In fact, as quoted by the Proponent, the Company announcement on December 20, 2013 stated:

“To the extent permitted by laws and regulations, AT&T’s transparency report will include:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.”

Subsequent to that announcement, the United States declassified certain information relating to its intelligence gathering, which AT&T relied on to issue a more extensive report than initially intended that complied with the law. Specifically, on January 27, 2014, the Director of National Intelligence de-classified certain specified aggregate data concerning requests for customer information consistent with the terms of the January 27, 2014 letter from the Deputy Attorney General.<sup>3</sup> In the DAG Letter, the Deputy Attorney General formally authorized communications providers to disclose this newly declassified information in one of two ways: “Option One” and “Option Two.” On February 17, 2014, AT&T published its first Transparency Report, which followed “Option One.” As discussed at length in the December 7 Submission and in the Sidley opinion, only because of these actions by the Director of National Intelligence and the Deputy Attorney General could the Company lawfully begin publishing transparency reports in 2014 that included aggregate data about FISA orders. As the Sidley opinion concluded, absent de-classification or other express authorization from the U.S. government to make the types of disclosures contemplated by the Proposal, the Company cannot do so without violating the law.<sup>4</sup>

---

<sup>3</sup> See Letter from James M. Cole, Deputy Attorney General, U.S. Department of Justice, to Colin Stretch, Esq., Vice President and General Counsel, Facebook, et al., Jan. 27, 2014, available at <http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf> (the “DAG Letter”); see also Sidley opinion at 4-6. We attach a copy of the DAG Letter to this letter as Exhibit A.

<sup>4</sup> See Sidley opinion at 5 (citing the Notice to the U.S. Foreign Intelligence Surveillance Court by the United States, *In re Amended Motion for Decl. Judgment*, Jan. 27, 2014, available at <http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf>).

***The January 5 Response Requests Non-Classified Information That Implicates the Company's Ordinary Business Operations.***

Second, to avoid the conclusion that the information called for by the Proposal is legally protected, the January 5 Response asks for new types of information not contemplated by the Proposal, which information, in any event, would be related to the Company's ordinary business operations. Relying on the Proposal's single reference to "law enforcement" cooperation as an example of non-classified information, the January 5 Response refers for the first time to disclosure of information regarding certain law enforcement agencies and activities under the so-called "Hemisphere Project" cited in a *New York Times* article, which reportedly relates to federal and local drug enforcement efforts. If the Proponent is interested in drug enforcement efforts by the government and the Company's assistance in such efforts, it is nowhere apparent in the Proposal, which is focused entirely on data privacy concerns in the context of intelligence gathering.

The January 5 Response is misleading to suggest that any shareholder would reasonably vote in favor of the Proposal in order to obtain disclosures about AT&T's cooperation with drug enforcement activity. The full text of the Proposal makes it clear that the Proposal's reference to "law enforcement" is with respect to the war on terrorism and intelligence gathering by the NSA and other intelligence gathering entities. The *New York Times* article cited in the Proposal does not relate to the Hemisphere Project but to the NSA, and no part of the Proposal suggests that the request relates to the Company's participation in drug enforcement efforts by the government.

To the extent the Company were to provide such information and other information that is not legally protected, the Proposal would fall squarely within AT&T's legal compliance program concerning its cooperation with local, state, and federal law enforcement, which is a matter of ordinary business and therefore excludable under Rule 14a-8(i)(7). The Staff has consistently recognized a company's legal compliance program as a matter of ordinary business and proposals relating to a company's compliance program as infringing on management's core function of overseeing business practices.<sup>5</sup>

---

<sup>5</sup> See *Navient Corp.* (Mar. 26, 2015); *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).

**CONCLUSION**

The Company, therefore, stands on the December 7 Submission and this supplemental letter for the reasons stated above. Accordingly, the Company continues to believe that the Proposal may be excluded from its 2016 Proxy Materials pursuant to Rule 14a-8(i)(2), 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](mailto: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,

  
Wayne Wirtz

Attachment: Exhibit A – DAG Letter

cc: Natasha Lamb, Arjuna Capital



Office of the Deputy Attorney General  
Washington, D.C. 20530

January 27, 2014

Sent via Email

Colin Stretch, Esquire  
Vice President and General Counsel  
Facebook Corporate Office  
1601 Willow Road  
Menlo Park, CA 94025

Kent Walker, Esquire  
Senior Vice President and General Counsel  
Google Corporate Office Headquarters  
1600 Amphitheater Parkway  
Mountain View, CA 94043

Erika Rottenberg, Esquire  
Vice President, General Counsel/Secretary  
LinkedIn Corporation  
2029 Stierlin Court  
Mountain View, CA 94043

Brad Smith, Esquire  
Executive Vice President and General Counsel  
Microsoft Corporate Office Headquarters  
One Microsoft Way  
Redmond, WA 98052-7329

Ronald Bell, Esquire  
General Counsel  
Yahoo Inc. Corporate Office and Headquarters  
701 First Avenue  
Sunnyvale, CA 94089

Dear General Counsels:

Pursuant to my discussions with you over the last month, this letter memorializes the new and additional ways in which the government will permit your company to report data concerning requests for customer information. We are sending this in connection with the Notice we filed with the Foreign Intelligence Surveillance Court today.

In the summer of 2013, the government agreed that providers could report in aggregate the total number of all requests received for customer data, including all criminal process, NSLs,

and FISA orders, and the total number of accounts targeted by those requests, in bands of 1000. In the alternative, the provider could separately report precise numbers of criminal process received and number of accounts affected thereby, as well as the number of NSLs received and the number of accounts affected thereby in bands of 1000. Under this latter option, however, a provider could not include in its reporting any data about FISA process received.

The government is now providing two alternative ways in which companies may inform their customers about requests for data. Consistent with the President's direction in his speech on January 17, 2014, these new reporting methods enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

Option One.

A provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The number of NSLs received, reported in bands of 1000 starting with 0-999.
3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.
4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.<sup>1</sup>
7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered

---

<sup>1</sup> As the Director of National Intelligence stated on November 18, 2013, the Government several years ago discontinued a program under which it collected bulk internet metadata, and no longer issues FISA orders for such information in bulk. See <http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence>. With regard to the bulk collection of telephone metadata, the President has ordered a transition that will end the Section 215 bulk metadata program as it currently exists and has requested recommendations about how the program should be restructured. The result of that transition will determine the manner in which data about any continued collection of that kind is most appropriately reported.

by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.

In addition, there will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a "New Capability Order" because disclosing it would reveal that the platform, product, or service is subject to previously undisclosed collection through FISA orders. For example, a report published on July 1, 2015, will not reflect data relating to any New Capability Order received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017. After data about a New Capability Order has been published, that type of order will no longer be considered a New Capability Order, and the ordinary six-month delay will apply.

The two-year delay described above does not apply to a FISA order directed at an enhancement to or iteration of an existing, already publicly available platform, product, or service when the company has received previously disclosed FISA orders of the same type for that platform, product, or service.

A provider may include in its transparency report general qualifying language regarding the existence of this additional delay mechanism to ensure the accuracy of its reported data, to the effect that the transparency report may or may not include orders subject to such additional delay (but without specifically confirming or denying that it has received such new capability orders).

#### Option Two.

In the alternative, a provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.
3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

\* \* \*

I have appreciated the opportunity to discuss these issues with you, and I am grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency. We look forward to continuing to discuss with you ways in which the

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell  
Page 4

government and industry can similarly find common ground on other issues raised by the surveillance debates of recent months.

Sincerely,

A handwritten signature in black ink, appearing to read 'James M. Cole', written in a cursive style.

James M. Cole  
Deputy Attorney General

January 5, 2016

VIA e-mail: [shareholderproposals@sec.gov](mailto:shareholderproposals@sec.gov)

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

Re: AT&T Inc.'s December 7, 2015 Request to Exclude Shareholder Proposal of Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss  
Securities and Exchange Act of 1934—Rule 14a-8

Dear Sir/Madam:

This letter is submitted on behalf of John Silva and Shana Weiss, as their designated representative in this matter, and (hereinafter referred to as the "Proponents"), who are beneficial owners of shares of common stock of AT&T Incorporated (hereinafter referred to as "AT&T" or the "Company"), and who have submitted a shareholder proposal (hereinafter referred to as "the Proposal") to AT&T, to respond to the letter dated December 7, 2015 sent to the Office of Chief Counsel by the Company, in which AT&T contends that the Proposal may be excluded from the Company's 2016 proxy statement under Rule 14a-8:

- Rule 14a-8(i)(2), because implementation of the Proposal by the Company would violate Federal law;
- Rule 14a-8(i)(7), because the Proposal deals with a matter relating to the Company's ordinary business operations; and
- Rule 14a-8(i)(10), because the Proposal has been substantially implemented by the Company, which has addressed the subject matter of the Proposal in existing reports and public disclosures.

We have reviewed the Company's letter and the contents of the Proposal, and it is our opinion that the Proposal should be included in AT&T's 2016 proxy statement because shareholders require a legal, transparent understanding of how AT&T is protecting the privacy of its customers.

### **Background**

In 2014, the Proponents co-filed a shareholder proposal asking AT&T to publish semi-annual transparency reports on government requests for customer information. The proposal was withdrawn after the Company agreed to publish the requested information. New information regarding the extent of AT&T's voluntary cooperation with government entities, despite the Company's own statement that "we do not provide information to any investigating authorities without a court order or other mandatory process other than if a person's life is in danger and time is of the essence," provides the basis of concern articulated in this proposal.

### **Shareholders Require Accountability, Transparency, and Clear Controls:**

AT&T and other telecom and Internet companies have been at the center of public concern and debate regarding the circumstances and conditions under which private customer information is shared with government and law enforcement entities. This issue has garnered significant attention from President Obama, Congress and the media, and poses a significant threat to business opportunities for the Company.

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. And yet, in August of this year *The New York Times* reported that as recently as 2013 the Company shared vast amounts of data with the National Security Agency (NSA) on a voluntary basis. It remains unclear how AT&T is providing, or has provided, information to both law enforcement and intelligence agencies, above and beyond what is legally required. These revelations regarding the extent to which AT&T and other telecommunication companies routinely provide metadata and call content to federal, state and local officials is of great concern to the public at large, as well as shareholders.

While AT&T seeks to exclude the proposal from going to a vote of shareholders, investors have a right of accountability to understand the Company's policies regarding the protection of customer information. The Proponents do not seek classified information, but a clear understanding of the Company's role in a controversy that spans nearly 15 years. Specifically, the proposal asks AT&T to clarify their policy of providing information to domestic and international law enforcement and intelligence agencies above and beyond what is legally required by court order or other legally mandated process.

The level of cooperation, or "partnership," between AT&T and government agencies, as described by an N.S.A official, is of great concern to the civil liberties of the Company's customers and as such, to the Company's shareholders. As our society rockets toward the era of Big Data, we cannot ignore the perennial threat of "Big Brother" and must draw clear and transparent lines between what is acceptable and unacceptable monitoring of our citizens', and AT&T's customers' communications. Indeed, society is most vulnerable to breaches of individual privacy in the wake of fear instilled by threats of terrorism and war. And while the attacks of September 11, 2001 set the stage for a new era of government surveillance and private sector partnership, we must not blindly accept a private/public police state without proper checks and balances. The Proponent's request of AT&T is one such check and balance and is essential to understand the Company's role in providing the government with customer information beyond its legal duty.

### **AT&T's Role in the Government Surveillance Controversy:**

Going back as far as 2001, AT&T has been the subject of controversy due to its role providing customer "metadata" to the federal government. The Harvard Business Review reported that over 40 lawsuits were filed against communication carriers, including AT&T, seeking "hundreds of billions of dollars in damages" alleging companies assisted the government with illegal wiretapping and data mining. AT&T was subsequently granted retroactive immunity by the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008. Since 2006, AT&T has been called out in the media, including the *Washington Post*, CNN, and the *New York Times* for altering its privacy policy to assume ownership of customer information, and to track customer location and web browsing. National Public Radio summarized:

AT&T is changing its privacy policy, ***to show that some customer information belongs to AT&T***. Privacy advocates say the company is trying to protect itself against future lawsuits for helping government eavesdroppers. But AT&T says it simply updated its policy to reflect technological changes, and its recent merger.<sup>1</sup>[emphasis added]

*The New York Times*, reporting on the customer location and web browsing policy change in 2009, noted that AT&T "can be forced to give all that information to the government without giving you the chance to object."

---

<sup>1</sup> <http://www.npr.org/templates/story/story.php?storyId:::5504560>

Further controversy includes AT&T's relationship with the Drug Enforcement Agency (DEA) in the Hemisphere Project. In 2013, the New York Times reported on a relationship going back to 2007, where the "government pays AT&T to place its employees in drug-fighting units across the country."<sup>2</sup> The relationship seemed to go beyond the arms length relationship between the Company and government agents customers might expect.

The extent of these relationships is of grave concern to the civil liberties of AT&T's customers and the Company's investors, who expect the business to operate within its social license.

### Analysis

#### **The proposal is not excludable under the ordinary business exclusion because Consumer Privacy is a Significant Social Policy Issue:**

AT&T goes so far as to say that such concerns relate simply to Ordinary Business, and therefore fall beyond the purview of shareholder involvement. To assert that the "protection of customer privacy is an ordinary business concern" in the wake of such intense public controversy over breaches of its customers' civil liberties is glib. The Commission has long recognized that proposals relating to social policy issues transcend day-to-day business matters and raise issues so significant that they must be allowed to face a shareholder vote.

Recent Staff communications indicate the use of several criteria in determining whether a matter *constitutes* a significant policy issue: level of public debate and controversy on the issue, media coverage, regulatory activity, and legislative and Presidential involvement. In addition, the Staff considers whether the subject matter constitutes a new issue or if it has ripened into a lasting public concern. In addition, it is *also* necessary for the proponent to demonstrate a *nexus* of the policy issue to the company.

In the present instance, the level of engagement by media, legislators, President Obama and the public on these issues of trust and transparency is exemplary of a significant policy issue.

Further, an issue which is not treated by the Staff as a significant policy issue in one year may ripen into such an issue. Indeed, the Staff originally treated another subject matter facing the same companies, net neutrality, as excludable ordinary business for several years. With growth in congressional and media interest, the issue was determined by the Staff to have ripened into a significant policy issue in 2012. With the present shareholder proposal, the same shift in treatment of the current subject matter is appropriate and necessary.

This is clearly a ripened issue. AT&T argues that "privacy" is an Ordinary Business Matter, citing cases which date back to 2009 and rely of prior instances when the Staff allowed ordinary business exclusions in its prior rulings on proposals similar to the current one. The reality is that times and circumstances have changed dramatically – and continue to change – in response to social, political and technological developments. The accumulated evidence *today* documents that this issue has attained the status of a high profile issue meeting all of the Staff's criteria for a significant policy issue.

This issue has occupied a great deal of public, media and congressional attention beginning at least as early as 2005. In 2015 alone, following extensive debate in Congress and widespread media attention, the

---

<sup>2</sup> Scott Shane, *Drug Agents Use Vast Phone Trove, Eclipsing NSA 's*, September 1, 2013. <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>

U.S. adopted two major laws affecting the relationship between U.S. government agencies and companies such as AT&T. These were the USA Freedom Act<sup>3</sup> (signed into law in June 2015) and the Cybersecurity Act of 2015<sup>4</sup> (which was included in the omnibus spending bill signed in December 2015). These new laws are in addition to proposed reforms of the 1986 Electronic Communications Privacy Act, which are now being considered by Congress.

The USA Freedom Act was the first piece of legislation to reform post 9/11 surveillance measures. "It's historical," said Sen. Patrick Leahy, D-Vermont, one of the leading architects of the reform efforts. "It's the first major overhaul of government surveillance in decades."

CNN reported: "The weeks-long buildup to the final vote was full of drama. Kentucky Sen. Rand Paul assailed the NSA in a 10-hour speech that roused civil libertarians around the country. He opposed both renewing the post 9/11-Patriot Act and the compromise measure -- that eventually passed -- known as the USA Freedom Act."<sup>5</sup>

The Cybersecurity Act of 2015 prompted similar intense public discussion and debate. The bill encourages companies to share cyber threat information with the government while providing them with liability protections.<sup>6</sup>

The National Journal noted debate across a wide political spectrum<sup>7</sup>:

"While business groups and national security hawks are cheering the news, it's a major blow to privacy advocates, who fear the measure will funnel more of Americans' personal information into the hands of the National Security Agency.

The legislation, now called the Cybersecurity Act of 2015, would encourage companies to share information about computer viruses and other cybersecurity threats with each other and the government. The bill would shield companies from lawsuits by their users for giving private information to the government as part of the program...

But civil-liberties groups warn the latest version of the measure has been stripped of some of the most significant privacy protections, transforming it into a surveillance bill."

More than 50 digital rights groups opposed the Cybersecurity Act on the grounds that it "seriously threatens privacy, civil liberties, and government accountability, and would undermine cybersecurity, rather than enhance it."<sup>8</sup>

Sean Doherty, president of TSC Advantage, an enterprise threat consultancy supporting Fortune 500 companies and the public sector, wrote in The Hill<sup>9</sup>:

---

<sup>3</sup> <https://www.washingtonpost.com/graphics/politics/usa-freedom-act/>

<sup>4</sup> <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/>

<sup>5</sup> <http://www.cnn.com/2015/06/02/politics/senate-usa-freedom-act-vote-patriot-act-nsa/>

<sup>6</sup> <http://www.usnews.com/news/articles/20151218/obamasignscybersecuritylawinspendingpackage>

<sup>7</sup> <http://www.nationaljournal.com/s/126185/controversial-cybersecurity-bill-poised-pass-massive-spending-package>

<sup>8</sup> [https://static.newamerica.org/attachments/1221851civilsocietygroupsandsecurityexpertstellcongresstheyopposecyberlegislation/FINAL\\_Civil\\_Society\\_Security\\_Expert\\_Letter%20Opposing\\_CSA\\_2015.efca7165edbf4beaa392e5ef66cfff70.pdf](https://static.newamerica.org/attachments/1221851civilsocietygroupsandsecurityexpertstellcongresstheyopposecyberlegislation/FINAL_Civil_Society_Security_Expert_Letter%20Opposing_CSA_2015.efca7165edbf4beaa392e5ef66cfff70.pdf)

While the government should be applauded for its determination to pass important cybersecurity legislation, businesses would be wise to proceed cautiously when considering whether to participate. It remains unclear what exactly will be defined as threat indicators, how information will be distributed among government agencies, and whether the privacy of citizens – in this case, the all-important customers of participating businesses - will be maintained.

And in the wake of the (December 2015) attack in San Bernardino, California, USA TODAY editorialized regarding calls for new sharing of data by telephone companies such as AT&T.<sup>10</sup>

Within days of the murder of 14 people in San Bernardino, Calif., by Islamic State sympathizers, a number of Republican senators are moving to resurrect a truly bad idea. Once again, they want to allow the National Security Agency to sweep up the phone records of virtually all Americans.

The once-secret "metadata" program, which a federal appeals court found amounted to "sweeping surveillance" of Americans' data in "staggering" volumes, ended in November, four days before the San Bernardino massacre. Now, some of the program's supporters are playing on the fears created by the California attack to try to bring the intrusive program back to life.

There are also calls for reform regarding other existing laws which affect disclosure of customer information by companies. In September 2015, the Senate Judiciary Committee held hearings regarding changes to the Electronic Privacy Communications Act. Brad Smith, President and Chief Legal Officer of Microsoft, wrote at the time on Microsoft's corporate blog:<sup>11</sup>

The good news is that hope is finally on the horizon. Legislation to reform ECPA and fix these problems now has swelling numbers of co-sponsors.

The reforms in this new legislation are sensible. For example, ECPA reform would require that a warrant be obtained by law enforcement before it can access the content of someone's email.

This would build on judicial trends and the fact that the courts increasingly agree that emails deserve the same protections as written letters in the physical world. In the groundbreaking Warshak case, a federal appellate court in fact ruled that law enforcement needs to get a warrant to get email content. The ECPA reform bill would codify this ruling.

A petition to President Obama, signed by 113 thousand U.S. citizens, called on the Administration "to support ECPA reform and to reject any special rules that would force online service providers to disclose our email without a warrant."<sup>12</sup>

And on the issue of encryption, AT&T's chief executive has acknowledged that the relationship between companies and law enforcement is indeed a policy issue. POLITICO reported in December 2015:

AT&T CEO Randall Stephenson wrote to employees last week, citing the renewed debate over encryption in the wake of the attacks in Paris in calling on the president and Congress to find a

---

<sup>9</sup> <http://thehill.com/blogs/congress-blog/technology/263635-approach-cyber-info-sharing-with-caution>

<sup>10</sup> [http://www.usatoday.com/story/opinion/2015/12/15/phone-metadata-nsa-san-bernardino-terrorists-attacks-isil-editorials-debates/76337140/?utm\\_source=NSHR+Rapid+Response&utm\\_campaign=c4aedac139-NSHR\\_Alerts\\_News\\_October\\_9&utm\\_medium=email&utm\\_term=0\\_3a915757be-c4aedac139-391774149](http://www.usatoday.com/story/opinion/2015/12/15/phone-metadata-nsa-san-bernardino-terrorists-attacks-isil-editorials-debates/76337140/?utm_source=NSHR+Rapid+Response&utm_campaign=c4aedac139-NSHR_Alerts_News_October_9&utm_medium=email&utm_term=0_3a915757be-c4aedac139-391774149)

<sup>11</sup> <http://blogs.microsoft.com/on-the-issues/2015/09/16/passing-ecpa-reform-it-has-never-been-more-important/>

<sup>12</sup> <https://petitions.whitehouse.gov/petition/reform-ecpa-tell-government-get-warrant>

balance between privacy and security. “We are firmly committed to the obligation we have to guard the personal privacy of the people we serve,” Stephenson wrote, according to a copy of the letter obtained by POLITICO. But “all companies must help law enforcement keep Americans safe by complying with valid court orders and legal warrants.” He called for a balance between competing interests but said it is up to policymakers, “not individual companies, to determine that balance.”<sup>13</sup>

**The proposal is not excludable as causing the Company to violate federal law:**

Contrary to the Company's arguments, the company would not be required to violate federal law in order to comply with the proposal. Even if we take the Company's questionable legal arguments on face value, that any disclosure that provides information on US intelligence operations is by definition classified information, the proposal still requests actions by the Company that would not disclose “classified information” as defined by the Company.

Reading the specific language of the proposal, it asks the company to “issue a report, at reasonable expense and excluding proprietary or legally protected information, clarifying the Company's 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.”

Further in its supporting statement the proposal requests that the report “should state what the Company is doing to ameliorate financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy “to the fullest extent possible.” The report should address the media reports that AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies. The report should also clarify whether information volunteered when “a person’s life is in danger and time is of the essence” includes ongoing data sharing arrangements.”

According to the Company's arguments, any disclosures providing information about US intelligence agencies should be considered to be classified information and therefore are not disclosable. This means that information on the Company's policies regarding providing information to US intelligence agencies is prohibited under federal law. However, the language of the proposal asks for quite a bit more disclosure than that category of disclosures. For instance, it requests disclosure of the same information regarding **law enforcement** agencies, which would include information relating to the controversial Hemisphere Project. *The New York Times* has reported:

The Hemisphere Project, a partnership between federal and local drug officials and AT&T that has not previously been reported, involves an extremely close association between the government and the telecommunications giant.

The government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987.

---

<sup>13</sup> : <http://www.politico.com/tipsheets/morning-cybersecurity/2015/12/chinese-in-dc-for-cyber-talks-is-the-plot-out-of-the-cyber-game-ukraine-cyber-war-the-book-211519#ixzz3vd0kWOIH>

Moreover, "intelligence agencies" domestically and internationally would include information sharing with non-US intelligence agencies, and therefore the Company could reasonably disclose changes in policies relating to those non-US intelligence agencies.

In addition, whether or not a particular disclosure regarding a change in policy would or would not disclose information relating to the operation of US intelligence agencies would seem to necessitate a case-by-case assessment. There is no evidence from the materials submitted by the Company that it has done such an assessment, but instead, they have merely made a blanket claim, obviously incorrect, that any information responsive to the proposal would violate federal law.

Finally, the Company's assertion that *any* discussion requested by the Proponent would violate federal law is a familiar argument – contradicted by the Company's own actions regarding Proponent's 2014 proposal. In a letter to the Staff dated December 5, 2013, the Company requested an exclusion of the Proponent's proposal at the time, noting that:

...because any information about assistance that AT&T has, or has not, provided to the government in connection with the government's foreign intelligence surveillance activities would almost certainly be classified information that AT&T could not legally disclose, the report sought in the Proposal, "subject to existing laws and regulation," would necessarily be limited to the Company's routine law enforcement compliance in the ordinary course of business.

Yet, only two weeks later, the Company announced that it would publish regular reports concerning government requests for confidential customer information. The Company said:

To further our efforts to be as transparent as possible within the government guidelines in which we operate, like Verizon recently announced, we intend to publish a semi-annual online report that will provide information on the number of law enforcement requests for customer information that our company receives in the countries in which we do business. AT&T expects to publish the first report, covering information received in 2013, in early 2014.

To the extent permitted by laws and regulations, AT&T's transparency report will include:

- The total number of law enforcement agency requests received from government authorities in criminal cases;
- Information on the number of subpoenas, court orders and warrants;
- The number of customers affected; and
- Details about the legal demands AT&T receives, as well as information about requests for information in emergencies.

**The proposal is not substantially implemented:**

In order for the Company to demonstrate substantial implementation it would need to show that it has fulfilled the guidelines of the proposal. Even if we assume that all information relating to US intelligence agencies is off-limits because it constitutes "legally protected information" so that the Company has already disclosed what it could regarding US agencies, the scope of the proposal still has extensive disclosure requests that are unfulfilled by the Company. These include the following, with regard to law enforcement agencies and non-US intelligence agencies:

- 1) Clarifying the Company's policies regarding sharing information with those agencies above and beyond what is legally required by court order or other legally mandated process, whether and

how those policies have changed since 2013, and assessing risks to the Company's finances and operations arising from current and past policies and practices. None of these aspects of the proposal have been fulfilled by existing disclosures or transparency reports.

- 2) Describing what the Company is doing to ameliorate financial and reputational risks raised by reports of the Company's behavior that appear inconsistent with its pledge to protect privacy to the fullest extent possible. Even with regard to disclosures relating to US intelligence agencies these damage control measures by the Company would seem to be disclosable.
- 3) Clarifying the circumstances in which the Company volunteers information to law enforcement or non-US intelligence agencies "when a person's life is in danger and time is of the essence," and specifically whether that includes ongoing data-sharing arrangements.

In light of the extensive information requested in the Proposal that is not fulfilled by the Company's existing reporting, the Company has not demonstrated that it has substantially implemented the proposal.

### Conclusion

The sharing of vast amounts of customer data gathered by AT&T with government entities, particularly on a voluntary basis, presents a threat to citizens' privacy and the Company's social license to operate. As society recognizes the threat Big Data presents in the context of an unchecked public private partnership, shareholders recognize that a failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks. The Company has not acted favorably on the contents of this proposal. We therefore call on the Company to clarify its role in providing information to government entities above and beyond its legal duty. 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 are providing a copy to AT&T's Associate General Counsel Wayne Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com).

Please contact me at (978) 578-4123 or [natasha@arjuna-capital.com](mailto:natasha@arjuna-capital.com) with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Natasha Lamb  
Director of Equity Research & Shareholder Engagement  
Arjuna Capital

cc: Wayne A. Wirtz via e-mail at [ww0118@att.com](mailto:ww0118@att.com)  
Associate General Counsel  
AT&T Incorporated



Wayne A. Wirtz  
AT&T Inc.  
Associate General Counsel  
208 S. Akard, Room 3024  
Dallas, Texas 75202  
(214) 757-3344  
ww0118@att.com

1934 Act/Rule 14a-8

December 7, 2015

***By email: [shareholderproposals@sec.gov](mailto: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: 2016 AT&T Inc. Annual Meeting of Shareholders  
Notice of Intent to Omit Shareholder Proposal of  
Arjuna Capital/Baldwin Brothers Inc. on behalf of  
John Silva and Shana Weiss Pursuant to Rule 14a-8

Ladies and Gentlemen:

Pursuant to Rule 14a-8(j) promulgated under the Securities Exchange Act of 1934, as amended, AT&T Inc., a Delaware corporation ("AT&T" or the "Company"), hereby notifies the Staff of the Division of Corporation Finance of the Securities and Exchange Commission of AT&T's intention to exclude a shareholder proposal submitted by Arjuna Capital/Baldwin Brothers Inc. (the "Proposal") on behalf of John Silva and Shana Weiss (the "Proponents") from its proxy materials for AT&T's 2016 Annual Meeting of Shareholders (the "2016 Proxy Materials").

This letter, together with the Proposal and the related correspondence, are being submitted to the Staff via e-mail in lieu of mailing paper copies. For the reasons stated below, AT&T intends to omit the Proposal from its 2016 Proxy Materials. A copy of this letter and the attachments are being sent on this date to the Proponents advising them of AT&T's intention to omit the Proposal from its 2016 Proxy Materials.

Rule 14a-8(k) provides that proponents are required to send companies a copy of any correspondence that the proponents elect to submit to the Commission or the Staff. Accordingly, we are taking this opportunity to inform the Proponents that if they elect to submit correspondence to the Commission or the Staff with respect to the Proposal, a copy of that correspondence must be furnished concurrently to the undersigned pursuant to Rule 14a-8(k) and *Staff Legal Bulletin 14D* (Nov. 7, 2008).

## INTRODUCTION AND BASES FOR EXCLUSION

The Proposal is entitled “Report on Surveillance Controversy.” After several paragraphs of introductory language, the Proposal sets forth the following resolution to be adopted by Company shareholders:

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

The Company believes that the Proposal may be properly excluded from the 2016 Proxy Materials pursuant to:

- Rule 14a-8(i)(2), because implementation of the Proposal by the Company would violate Federal law;
- Rule 14a-8(i)(7), because the Proposal deals with a matter relating to the Company’s ordinary business operations; and
- Rule 14a-8(i)(10), because the Proposal has been substantially implemented by the Company, which has addressed the subject matter of the Proposal in existing reports and public disclosures.

## THE PROPOSAL

The Proposal, in its entirety, reads as follows:

### “Report on Surveillance Controversy

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, an August 2015 *New York Times* article disclosed new documents alleging that as recently as 2013 the company shared 60 million foreign-to-foreign emails a day with the National Security Agency (NSA), on a voluntary basis, not required by court order.

The *Times* article states:

One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, “This is a partnership, not a contractual relationship.”

AT&T spokesman Brad Burns has stated, “we do not provide information to any investigating authorities without a court order or other mandatory process other than if a person's life is in danger and time is of the essence.”

Responding to growing public concern over these issues, AT&T issued transparency reports, but the reports do not address specific concerns raised regarding the foreign emails and implications for international business plans.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program “a breach of international law.” U.S. Senator Ron Wyden said, “I have to believe the civil liberties of millions of American have been violated.” The *Wall Street Journal* has reported that AT&T’s plans to expand its mobile network in Europe, including anticipated acquisitions, could face “unexpected hurdles” due to its cooperation with NSA consumer information requests.

The Information Technology and Innovation Foundation estimates that the negative economic impact of U.S. surveillance practices will likely “far exceed” its 2013 estimate of 35 billion dollars, largely because “foreign customers are shunning U.S. companies.”

While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

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

**Supporting Statement:**

**The Proponent believes the report should state what the Company is doing to ameliorate financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy “to the fullest extent possible.” The report should address the media reports that AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies. The report should also clarify whether information volunteered when “a person’s life is in danger and time is of the essence” includes ongoing data sharing arrangements.”**

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

## ARGUMENT

### ***A. The Proposal May Be Properly Omitted From the 2016 Proxy Materials Pursuant to Rule 14a-8(i)(2) Because Implementation of the Proposal by the Company Would Violate Federal Law.***

A shareholder proposal may be properly omitted pursuant to Rule 14a-8(i)(2) if it would, upon implementation, “cause the company to violate any state, federal or foreign law to which is it subject.” The Company believes the Proposal may be excluded from the 2016 Proxy Materials on this basis. We have set forth above the Proposal in its entirety to show how it focuses on surveillance and the alleged voluntary cooperation between the Company and the National Security Agency (“NSA”) and other government intelligence agencies. The “Resolved” clause requests a report “clarifying the Company’s 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.” The “Supporting Statement” specifies that the report requested by the Proposal should “state what the Company is doing to ameliorate financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy ‘to the fullest extent possible’” and should “address the media reports that AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies.” Although the “Resolved” clause also mentions “law enforcement,” there is no indication in the rest of the Proposal why law enforcement is included, since the remaining 489 words of the Proposal focus on surveillance and the Company’s allegedly providing information to NSA “above and beyond what is legally required by court order or other legally mandated process.”

Although the “Resolved” clause provides that the requested report may be prepared by the Company in a manner that excludes “proprietary or legally protected information,” given the focus of the Proposal, AT&T does not believe that it could implement the Proposal in a manner consistent with shareholders’ expectations without, at minimum, either confirming or denying whether it provides information to the NSA “above and beyond what is legally required by court order or other legally mandated process.” AT&T has obtained a legal opinion from the law firm of Sidley Austin LLP (the “Sidley Opinion”)<sup>1</sup> that opines that it would be impossible for AT&T to produce the report called for by the Proposal without providing information that the United States has deemed classified and over which it has asserted its state secrets privilege. Therefore, according to the Sidley Opinion, implementing the Proposal would cause AT&T to violate federal laws intended to protect the intelligence-gathering activities of the United States,

---

<sup>1</sup> The Sidley Opinion is attached to this letter as Exhibit B.

including 18 U.S.C. § 798(a), which specifically prohibits knowingly and willfully divulging to an unauthorized person classified information regarding the communications intelligence activities of the United States. As this analysis is discussed in the Sidley Opinion, such discussion is incorporated in this letter and will not be repeated here. It is important to note that AT&T has neither confirmed nor denied the existence of any of the activities that are the basis of the Proposal nor does AT&T now confirm or deny that it has participated in any such activities.

Since implementation of the Proposal would require AT&T to violate federal law, AT&T may properly exclude the Proposal from its 2016 Proxy Materials in accordance with Rule 14a-8(i)(2).

***B. The Proposal May Be Properly Omitted From the 2016 Proxy Materials Pursuant to Rule 14a-8(i)(7) Because It Deals With a Matter Involving the Company's Ordinary Business Operations***

Paragraph (i)(7) of Rule 14a-8 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 general policy underlying 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 stockholders meeting."<sup>2</sup> Two central considerations underlie this basis for omission. *First*, "[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."<sup>3</sup> *Second*, 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 be in a position to make an informed judgment."<sup>4</sup>

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.<sup>5</sup> In other words, the critical element is the nature of the matters that are the ultimate focus of the proposal, *not* the fact that the proposal might be styled as a request for a report or study or a policy discussion by a company, its board of directors or anyone else. The United States Court of Appeals for the Third Circuit recently underscored the importance of this distinction in *Trinity Wall Street v. Wal-Mart Stores, Inc.*, noting the Commission's "consistent nod to substance over form and its distaste for clever drafting in evaluating stockholder proposals" and emphasized that "it matters little how a shareholder styles its proposal; the emphasis should always be on its substance."<sup>6</sup> The Third

<sup>2</sup> Release No. 34-40018 (May 21, 1998) (the "1998 Release").

<sup>3</sup> *Ibid.*

<sup>4</sup> *Ibid.*

<sup>5</sup> Release No. 34-20091 (Aug. 16, 1983).

<sup>6</sup> 792 F.3d 323, 341 (3d Cir. 2015).

Circuit in *Trinity* also took judicial notice of Staff grants of no-action relief in circumstances where shareholder proponents sought reports on the company's exposure to certain risks, but the underlying subject matter of the risks involved ordinary business matters.<sup>7</sup>

*Protection of Customer Privacy Is an Ordinary Business Matter*

The 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, as described above. 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 connection with its annual meetings in 2007 and 2008, the Company received proposals similar to the Proponent's, and in both cases the Staff issued a no-action letter confirming it would not recommend any enforcement action if the Company excluded the proposals from its annual proxy materials because the proposals related to the Company's ordinary business operations.

Of particular relevance to the current Proposal, the 2008 meeting proposal requested the preparation of a report about policy issues relating to the disclosure of customer records and the content of customer communications to federal and state governmental agencies without a warrant.<sup>8</sup> The Staff issued a no-action letter stating it would not object if the Company excluded the proposal on the ground that "it related to AT&T's ordinary business operations (*i.e.*, procedures for *protecting customer information*)."<sup>9</sup>

The Staff has also issued no-action letters 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.<sup>10</sup> In addition, the Staff has recognized customer privacy as an ordinary business matter for companies outside the telecommunications industry.<sup>11</sup> For the purpose of paragraph (i)(7) of the Rule, there is no

---

<sup>7</sup> *Ibid.* at 342-343, citing *Sempra Energy* (Jan. 12, 2012) (granting no-action relief where the proposal requested Board review of the political, legal and financial risks relating to the company's operations in countries where corrupt practices may be more prominent); *The Home Depot, Inc.* (Jan. 25, 2008) (granting no-action relief where the proposal asked the board to publish a report outlining the company's product safety policies and describing management's efforts address recent product safety concerns); and *Family Dollar Stores* (Nov. 6, 2007) (granting no-action relief where the proposal asked for a report evaluating the company's policies and procedures for systematically minimizing customers' exposure to toxic substances and hazardous components in its marketed materials). Each of these letters emphasized that, while the proposal sought a report or review, the underlying subject matter of the request appeared to involve ordinary business matters.

<sup>8</sup> *AT&T Inc.* (Feb. 7, 2008).

<sup>9</sup> *Ibid.* (emphasis added). The 2007 meeting proposal also requested the preparation of a report regarding disclosure of customer communications and related information to specified governmental agencies (including the National Security Agency) without a warrant. *AT&T Inc.* (February 9, 2007). In addition, in 2009, the Company received a meeting proposal relating to 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).

<sup>10</sup> See, e.g., *Sprint Nextel Corporation* (Feb. 17, 2009); *Verizon Communications Inc.* (Feb. 22, 2007).

<sup>11</sup> 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

credible way to distinguish the customer privacy matters that were the focus of these prior excluded proposals from the customer privacy matters that are the focus of the current Proposal: all are ordinary business matters.

To require inclusion of proposals that address such complex and fundamental matters as customer privacy would disregard the critical dividing line between management and shareholder functions. The Staff has long recognized that companies need not include shareholder proposals that seek to micro-manage a company's business.

*The Proposal Relates to Matters of Legal Compliance*

The Proposal may also be properly excluded pursuant to paragraph (i)(7) because it implicates the Company's conduct of its legal compliance program. The Staff has long identified a company's compliance with laws and regulations as a matter of ordinary business. The Staff recently permitted Navient Corporation to exclude a proposal recommending that it prepare a report on its internal controls over its student loan servicing operations, including a discussion of the actions taken to ensure compliance with applicable law.<sup>12</sup> 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)." The Proposal plainly seeks clarification of the Company's existing legal compliance program relating to the provision of information to law enforcement and intelligence agencies; it is impossible to dissociate the information sought by the Proposal from the Company's legal compliance program relating to the provision of information to governmental agencies.

***C. The Proposal Has Been Substantially Implemented and May Be Excluded Pursuant to Exchange Act Rule 14a-8(i)(10)***

Paragraph (i)(10) of Rule 14a-8 permits the exclusion of a shareholder proposal from a company's proxy statement 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."<sup>13</sup>

A shareholder proposal is considered to be substantially implemented if the company's relevant "policies, practices and procedures compare favorably with the guidelines of the proposal."<sup>14</sup> The Staff does not require that a company implement every detail of a proposal in order to permit exclusion under Rule 14a-8(i)(10). Rather, the Staff has consistently permitted

---

policies and procedures for ensuring the confidentiality of customer information could be excluded as relating to ordinary business matters).

<sup>12</sup> *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).

<sup>13</sup> Exchange Act Release No. 20091 (Aug. 16, 1983).

<sup>14</sup> *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).

exclusion of a shareholder proposal when a company already has policies and procedures in place relating to the subject matter of the shareholder proposal, or has implemented the essential objectives of the shareholder proposal.<sup>15</sup>

The Staff has also established that a company does not have to implement every detail of a proposal in order to exclude it under paragraph (i)(10) of Rule 14a-8. Rather, “substantial implementation” requires only that the company’s actions satisfactorily address the underlying concerns of the proposal.<sup>16</sup>

*The Company Has Substantially Implemented the Proposal Through Existing Policies, Procedures and Reports*

As noted above, the Proposal focuses on the Company’s policies regarding the provision of customer information to law enforcement and intelligence 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 as well as the Company’s responses to those demands.<sup>17</sup> The core of any report prepared in response to the Proposal would be based upon the existing Transparency Reports. Each Transparency Report contains, to the extent permitted by law:

- the total number of National Securities Letters and Foreign Intelligence Surveillance Act (“FISA”) orders received and the number of customer accounts affected;<sup>18</sup>

---

<sup>15</sup> See, e.g., *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 excluded where existing company laboratory animal care guidelines and policy were available on its website); *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 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 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 excluded in light of the company’s own business practice standards).

<sup>16</sup> *Masco Corp.* (Mar. 29, 1999); see also, e.g., *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).

<sup>17</sup> The Transparency Reports are available at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>.

<sup>18</sup> The reported FISA orders information has been tailored to comply with one of the two permissible methods of reporting aggregated FISA orders that the U.S. Deputy Attorney General outlined in a January 27, 2014 letter, which the U.S. Department of Justice indicated were issued “to allow more detailed disclosures about the number of national security orders and requests issued to communications providers, and the number of customer accounts targeted under those orders and requests including the underlying legal authorities.” Letter from James M. Cole, Deputy Attorney General, U.S. Department of Justice, to Colin Stretch, Vice President and General Counsel, Facebook *et al.* (Jan. 27, 2014), <http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf>; Joint Statement by Attorney General Eric Holder and Director of National Intelligence James Clapper on New Reporting Methods for National Security Orders, Jan. 27, 2014, <http://www.justice.gov/opa/pr/joint-statement-attorney-general-eric-holder-and-director-national-intelligence-james-clapper>.

- 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 emergency requests received; and
- the total number of international demands received.<sup>19</sup>

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 5 through 9 of the Transparency Report that AT&T published for the first six-month period in 2015. AT&T has also adopted a Privacy Policy, appointed a Chief Privacy Officer and trained relevant employees on compliance with the Privacy Policy.<sup>20</sup> The Privacy Policy, among other things, describes the Company's practices and procedures for protecting the confidentiality of customer information and how the Company implements and updates them. Among other things, the Company posts publicly on its website prominent notices of important pending changes at least 30 days before the effective date.<sup>21</sup>

It is worth noting that in December 2013, the Proponent, together with certain other proponents, submitted a proposal requesting that the Company "publish semi-annual reports, subject to existing laws and regulations, providing metrics and discussion regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information." In January 2014, the Company published its first Transparency Report. The proponents of that proposal voluntarily withdrew it in light of the Company's publication of the report (before the Staff issued a ruling on the Company's no-action request relating to the December 2013 proposal). The Proponent's latest proposal represents an incremental request for disclosure regarding the same policies and procedures that the Proponent sought and the Company provided just two years ago, and presents a trend of seeking shareholder votes on ever-increasing disclosure by recalibrating the scope of requested disclosure on the same subject.

\* \* \* \*

For the reasons set forth in this letter, we respectfully request the Staff concur that the Company may properly omit the Proposal from its 2016 Proxy Materials in reliance on Rule 14a-8. If you would like to discuss this request, please feel free to contact the undersigned by telephone at (214) 757-3344 or Thomas Kim, Esq., of Sidley Austin LLP at (202) 736-8615.

Sincerely,



---

<sup>19</sup> *Ibid.*

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

<sup>21</sup> *Ibid.*

Enclosures

cc: Natasha Lamb  
(Arjuna Capital/Baldwin Brothers Inc.)

# EXHIBIT A

**LUTHY, KATHERINE J (Legal)**

---

**From:** Natasha Lamb <natasha@arjuna-capital.com>  
**Sent:** Wednesday, November 11, 2015 11:42 AM  
**To:** stacey.maris@att.com; s.maris@att.com  
**Cc:** LUTHY, KATHERINE J (Legal); WIRTZ, WAYNE A (Legal); STEPHENSON, RANDALL  
**Subject:** Shareholder Proposal  
**Attachments:** 01B95DEB-FA3E-46F7-BBC0-22120BCE7DB9[47].png; AT&T Revised Proposal.pdf

**Importance:** High

Dear Ms. Maris,

I am submitting the attached proposal as an amendment/revision to be substituted for the version mailed to your office today. I look forward to speaking with you about the content of our proposal.

Sincerely,  
Natasha Lamb

[esig\_natasha.gif]

## **Report on Surveillance Controversy**

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, an August 2015 *New York Times* article disclosed new documents alleging that as recently as 2013 the company shared 60 million foreign-to-foreign emails a day with the National Security Agency (NSA), on a voluntary basis, not required by court order.

The *Times* article states:

One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, "This is a partnership, not a contractual relationship."

AT&T spokesman Brad Burns has stated, "we do not provide information to any investigating authorities without a court order or other mandatory process other than if a person's life is in danger and time is of the essence."

Responding to growing public concern over these issues, AT&T issued transparency reports, but the reports do not address specific concerns raised regarding the foreign emails and implications for international business plans.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of American have been violated." The *Wall Street Journal* has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its cooperation with NSA consumer information requests.

The Information Technology and Innovation Foundation estimates that the negative economic impact of U.S. surveillance practices will likely "far exceed" its 2013 estimate of 35 billion dollars, largely because "foreign customers are shunning U.S. companies."

While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

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

**Supporting Statement:**

**The Proponent believes the report should state what the Company is doing to ameliorate financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy "to the fullest extent possible." The report should address the media reports that AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies. The report should also clarify whether information volunteered when "a person's life is in danger and time is of the essence" includes ongoing data sharing arrangements.**

# EXHIBIT B



SIDLEY AUSTIN LLP  
 1501 K STREET, N.W.  
 WASHINGTON, D.C. 20005  
 (202) 736 8000  
 (202) 736 8711 FAX

BEIJING	HONG KONG	SHANGHAI
BOSTON	HOUSTON	SINGAPORE
BRUSSELS	LONDON	SYDNEY
CHICAGO	LOS ANGELES	TOKYO
DALLAS	NEW YORK	WASHINGTON, D.C.
FRANKFURT	PALO ALTO	
GENEVA	SAN FRANCISCO	

FOUNDED 1866

December 7, 2015

Board of Directors  
 AT&T Inc.  
 c/o David R. McAtee II, Esq.  
 Senior Executive Vice President and  
 General Counsel  
 208 South Akard Street  
 Dallas, TX 75202

Re: Arjuna Capital/Baldwin Brothers Inc. Proposal

Ladies and Gentlemen:

You have requested our legal opinion as to whether AT&T Inc. (“AT&T” or the “Company”) would violate federal law if it were to implement the shareholder proposal (the “Proposal”) submitted by Arjuna Capital/Baldwin Brothers Inc. on behalf of John Silva and Shana Weiss (collectively, the “Proponent”) for inclusion in the Company’s proxy statement and form of proxy for its 2016 Annual Meeting of Shareholders (“2016 Proxy Materials”).

**The Proposal.** The Proposal calls for AT&T to issue a report (1) “clarifying the Company’s 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”; (2) explaining “whether and how the policies have changed since 2013”; and (3) “assessing risks to the Company’s finances and operations arising from current and past policies and practices.”<sup>1</sup> Any such report, among other things, should also address media reports that “AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies.”

**I. Analysis and Discussion**

**A. Applicable Legal Framework.** *Federal Criminal Prohibition On Disclosure Of Classified Information Concerning The Communication Intelligence Activities Of The United States.* It is a felony under federal law to knowingly and willfully divulge to an unauthorized

<sup>1</sup> A copy of the Proposal is enclosed with this Opinion as an Exhibit.

person classified information regarding the communications intelligence activities of the United States. In particular, 18 U.S.C. § 798(a) provides:

Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States, or for the benefit of any foreign government to the detriment of the United States any classified information –

\* \* \* \*

- (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
- (3) concerning the communication intelligence activities of the United States or any foreign government...

\* \* \* \*

Shall be fined under this title or imprisoned not more than ten years, or both.

As defined by this statute, the term “classified information” means “information which, at the time of a violation of this section, is for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution....”<sup>2</sup> The term “unauthorized person” means “any person, who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government to engage in communication intelligence activities for the United States.”<sup>3</sup>

The Proposal makes express reference to the alleged signals intelligence activities – “foreign-to-foreign email traffic” – of the National Security Agency (“NSA”). Section 6 of the National Security Agency Act, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides that “nothing in this Act or any other law...shall be construed to require the

---

<sup>2</sup> 18 U.S.C. § 798(b).

<sup>3</sup> *Id.*

disclosure of the organization or any function of the National Security Agency, or of any information with respect to the activities thereof . . .”). These restrictions are categorical and “absolute.”<sup>4</sup> Accordingly, they exist regardless of whether any involvement in these activities is voluntary or compelled and without limitation as to “any other law.”

**B. Assessment of Legality of Proposal.**

AT&T cannot legally provide the report requested by the Proposal. The Proposal requests information about AT&T’s dealings with the NSA and foreign intelligence agencies – specifically, information about the Company’s 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,” as well as responses to the allegations in media reports, including the *New York Times*, that the Company “provided NSA access to foreign-to-foreign email traffic and . . . to Internet traffic that AT&T transmits for other telecom companies.”

Like every other entity, AT&T is barred by 18 U.S.C. § 798(a) and Section 6 of the National Security Agency Act (the “Referenced Federal Statutes”), as cited above, from disclosing classified information “concerning the communication intelligence activities of the United States or any foreign government” and about “any function of the National Security Agency, or of any information with respect to the activities thereof.” As the U.S. Department of Justice (“DOJ”) has explained in its response to suits brought by several Internet companies in the U.S. Foreign Intelligence Surveillance Court seeking declaratory relief to disclose aggregate Foreign Intelligence Surveillance Act (“FISA”) orders (the “FISA Litigation”), classified information encompasses more than the contents of any requests (such as the identity of the surveillance target) that a communications provider might have received pursuant to FISA. Rather, classified information also includes the “sources and methods of surveillance.”<sup>5</sup> This prohibition exists regardless of whether the sources or methods are voluntarily provided or compelled by law.

The Proposal is premised on the view that the disclosure of a policy regarding providing information to NSA and foreign intelligence agencies “above and beyond what is legally

---

<sup>4</sup> *Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996) (“[t]he protection afforded by section 6 is, by its very terms, absolute”); see also *Founding Church of Scientology v. National Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden v. National Security Agency*, 608 F.2d 1381, 1390 (D.C. Cir. 1979).

<sup>5</sup> Resp. of the United States to Motions for Declaratory Judgment By Google Inc. *et al.*, at 4, *In re Amended Motion for Decl. Judgment*, Docket Nos. 13-03, *et al.* (FISA Ct. filed Sept. 30. 2013) (“DOJ Metrics Response”).

required by court order or other legally mandated process,” including whether AT&T provides the NSA with access to Internet traffic that AT&T transmit for other telecom companies and to foreign-to-foreign emails, is not, in and of itself, classified information. However, as the DOJ has explained in the FISA Litigation, this:

“implausible reading ignores the forest for the trees. It would permit damaging disclosures that would reveal sources and methods of surveillance potentially nationwide. The secrecy provisions in the [FISA] orders flow from statutory requirements that, according to their plain language, protect such sources and methods, not just particular collection efforts.”<sup>6</sup>

In other words, disclosure about whether and the extent to which, if any, AT&T provides information to the NSA “would provide adversaries significant information about the Government’s collection capabilities with respect to particular providers” – and thereby provide adversaries a guide to avoiding surveillance.<sup>7</sup> To the extent any such information exists, it would be classified and thus illegal to reveal.

In addition, it is well established that the government’s decision to classify information is subject to “utmost deference.”<sup>8</sup> This deference is especially strong in areas of national defense and foreign policy.<sup>9</sup> With respect to information about the NSA’s activities: in January 2014, to settle the FISA Litigation, the DOJ announced that the Obama Administration was “acting to

---

<sup>6</sup> DOJ Metrics Response at 4. *See also id.* at 3 (if providers revealed “the nature and scope of any FISA surveillance of their communications platforms,” such disclosures “would be invaluable to our adversaries, who could thereby derive a clear picture of where the Government’s surveillance efforts are directed and how its surveillance activities change over time, including when the Government initiates or expands surveillance efforts involving providers or services that adversaries previously considered ‘safe.’”).

<sup>7</sup> *Id.* at 3-7, 9.

<sup>8</sup> *Department of the Navy v. Egan*, 484 U.S. 518, 529-30 (1988); *see id.* at 529 (“For ‘reasons . . . too obvious to call for enlarged discussion,’ the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it.”) (*quoting CIA v. Sims*, 471 U.S. 159, 170 (1985)).

<sup>9</sup> *See, e.g., Larson v. Dep’t of State*, 565 F.3d 857, 864 (D.C. Cir. 2009) (courts “accord substantial weight to an agency’s affidavit concerning the details of the classified status of [a] disputed record because the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse [e]ffects might occur as a result of a particular classified record”); *Krikorian v. Dep’t of State*, 984 F.2d 461, 464-65 (D.C. Cir. 1993) (courts “lack the expertise” to “second-guess [] agency opinions” in the “typical national security . . . case” seeking disclosure of classified material).

allow more detailed disclosures about the number of national security orders and requests issued to communications providers, and the number of customer accounts targeted under those orders and requests including the underlying legal authorities.”<sup>10</sup> Specifically, in a letter dated January 27, 2014, the Deputy Attorney General outlined two new reporting methods whereby communications providers could make public aggregate data about FISA orders (the “DAG Letter”).<sup>11</sup> Correspondingly, the Director of National Intelligence declassified aggregate data about FISA orders consistent with the terms of the DAG Letter. In submitting the DAG Letter to the U.S. Foreign Intelligence Surveillance Court, the DOJ indicated that the “Government will therefore treat such disclosures as no longer prohibited under any legal provision that would otherwise prohibit the disclosure of classified data, including data relating to FISA surveillance. *It is the Government’s position that the terms outlined in the Deputy Attorney General’s letter define the limits of permissible reporting for the parties and other similarly situated companies*”<sup>12</sup> (emphasis added).

---

<sup>10</sup> Joint Statement by Attorney General Eric Holder and Director of National Intelligence James Clapper on New Reporting Methods for National Security Orders, Jan. 27, 2014, available at <http://www.justice.gov/opa/pr/joint-statement-attorney-general-eric-holder-and-director-national-intelligence-james-clapper>.

<sup>11</sup> Letter from James M. Cole, Deputy Attorney General, U.S. Department of Justice, to Colin Stretch, Vice President and General Counsel, Facebook et al. (Jan. 27, 2014), available at <http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf>.

Following the guidance in the DAG Letter, in 2014, AT&T began publishing transparency reports disclosing requests for customer information – including pursuant to National Security Letters and FISA orders, as well as U.S. criminal and civil demands – that AT&T has received in the United States and the other countries in which it does business (the “AT&T Transparency Reports”). AT&T publishes and updates these reports semi-annually. Each AT&T Transparency Report includes, to the extent permitted by laws and regulations:

- the total number of National Securities Letters and FISA orders received and the number of customer accounts affected;
- 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 emergency requests received; and
- the total number of international demands received.

Available at

[http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT\\_Transparency%20Report\\_July%202015.pdf](http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT_Transparency%20Report_July%202015.pdf)

<sup>12</sup> Notice to the U.S. Foreign Intelligence Surveillance Court by the United States, *In re Amended Motion for Decl. Judgment*, Jan. 27, 2014 (the “Notice”), available at <http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf>.

Disclosure of information outside of these limits – such as whether and the extent to which, if any, AT&T voluntarily provides information to the NSA or information about whether AT&T grants the NSA access to foreign-to-foreign email traffic or to Internet traffic that AT&T transmits for other telecom companies – would be subject to “any legal provision that would otherwise prohibit the disclosure of classified data, including data relating to FISA surveillance.”<sup>13</sup> In our opinion, consistent with the DAG Letter, which necessitated the Director of National Intelligence declassifying aggregated data disclosed consistent with the terms of the DAG Letter, the United States would view disclosures of matters about AT&T’s policies regarding providing information to the NSA and other intelligence agencies “above and beyond what is legally required by court order or other legally mandated process” or of responses to the media reports stating that AT&T provided NSA access to foreign-to-foreign email traffic and to Internet traffic that AT&T transmits for other telecom companies as unlawful disclosures of classified information.

*Irrelevance of Proponent’s Qualification.* The legality of the Proposal is not affected by Proponent’s qualification that AT&T may exclude from the report any “legally protected information.”

The Proposal expressly requests disclosure of classified information, to the extent it exists, regarding the NSA and information about any involvement – voluntary or compulsory – of AT&T in the signals intelligence activities of the NSA. AT&T could not implement the Proposal consistent with shareholders’ expectations without at least implicitly providing information that would confirm or deny whether the allegations about AT&T’s dealings with the NSA and foreign intelligence agencies are true – all of which the United States considers classified information.

## II. Opinion.

In rendering our opinion, we have considered the applicable provisions of the United States Code, relevant judicial interpretations, and such other legal authorities as we have considered relevant. It should be noted that such statutes, interpretations, and other authorities are subject to change. Any such changes may be retroactive and could have an effect on the conclusions stated herein.<sup>14</sup>

---

<sup>13</sup> See Notice.

<sup>14</sup> We have assumed the genuineness of all signatures, the proper filing of all documents which purport to be filed with federal agencies, the legal capacity of all natural persons to sign such documents, the authenticity of all documents submitted to us as originals and the conformity with the original documents of all documents submitted to us by electronic transmission.



Board of Directors  
December 7, 2015  
Page 7

Based on the foregoing facts and analysis regarding the Proposal as recited herein, and subject to the qualifications, assumptions and discussions contained herein, we are of the opinion that the AT&T would violate the Referenced Federal Statutes if it were to implement the Proposal.<sup>15</sup>

Sincerely,

A handwritten signature in cursive script that reads "Sidley Austin LLP".

Sidley Austin LLP

Attachment: Exhibit – copy of the Proposal

---

<sup>15</sup> Our analysis is limited to the facts and assumptions as they are presented herein and is subject to the qualification that there are no additional facts that would materially affect the validity of the assumptions and conclusions set forth herein or upon which this opinion is based. Our conclusions are based on the law specifically referenced here as of the date hereof; we express no opinion as to the laws, rules or regulations not specifically referenced; and we assume no obligation to advise you of changes in the law, facts or other circumstances (or the effect thereof on the opinion expressed or the statements made herein) that hereafter may come to our attention. The foregoing assessment is not intended to be a guarantee as to what a particular court would actually hold, but an assessment of a reviewing court's action if the issues were properly presented to it and the court followed what we believe to be the applicable legal principles. This opinion may not be relied upon in whole or in part by any other person or entity other than its addressee without our specific prior written consent. We understand that you intend to attach a copy of this opinion to a letter relating to the Proposal to the SEC's Division of Corporation Finance pursuant to the procedures set forth in 17 C.F.R. § 240.14a-8, and we hereby consent to the use of this opinion for that purpose.

**EXHIBIT**

## Report on Surveillance Controversy

AT&T acknowledges in its corporate code of conduct that privacy is critical to the success of its business. Yet, an August 2015 *New York Times* article disclosed new documents alleging that as recently as 2013 the company shared 60 million foreign-to-foreign emails a day with the National Security Agency (NSA), on a voluntary basis, not required by court order.

The *Times* article states:

One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, "This is a partnership, not a contractual relationship."

AT&T spokesman Brad Burns has stated, "we do not provide information to any investigating authorities without a court order or other mandatory process other than if a person's life is in danger and time is of the essence."

Responding to growing public concern over these issues, AT&T issued transparency reports, but the reports do not address specific concerns raised regarding the foreign emails and implications for international business plans.

Controversy over U.S. government surveillance programs reportedly involving AT&T has spurred massive global press coverage, hearings in the U.S. Congress and the European legislature, and widespread calls for reform. Brazilian President Dilma Rousseff called the NSA surveillance program "a breach of international law." U.S. Senator Ron Wyden said, "I have to believe the civil liberties of millions of American have been violated." The *Wall Street Journal* has reported that AT&T's plans to expand its mobile network in Europe, including anticipated acquisitions, could face "unexpected hurdles" due to its cooperation with NSA consumer information requests.

The Information Technology and Innovation Foundation estimates that the negative economic impact of U.S. surveillance practices will likely "far exceed" its 2013 estimate of 35 billion dollars, largely because "foreign customers are shunning U.S. companies."

While AT&T must comply with its legal obligations, failure to persuade customers of a genuine and long-term commitment to privacy rights could present AT&T with serious financial, legal and reputational risks.

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

**Supporting Statement:**

The Proponent believes the report should state what the Company is doing to ameliorate financial and reputational risks raised by reports of AT&T behavior that appear inconsistent with its pledge to protect privacy "to the fullest extent possible." The report should address the media reports that AT&T provided NSA access to foreign-to-foreign email traffic and, according to a former employee, to Internet traffic that AT&T transmits for other telecom companies. The report should also clarify whether information volunteered when "a person's life is in danger and time is of the essence" includes ongoing data sharing arrangements.