Jan Witold Baran
202.719.7330
jbaran@wileyrein.com

BY HAND DELIVERY

August 21, 2018

Federal Election Commission
1050 First Street, NE
Washington, DC 20463

Re: Advisory Opinion Request (Microsoft Corporation)

Dear Commissioners:

On behalf of Microsoft Corporation ("Microsoft"), we request an advisory opinion from the Federal Election Commission ("Commission" or "FEC") pursuant to 52 U.S.C. § 30108 of the Federal Election Campaign Act of 1971, as amended (the "Act"). Specifically, we seek confirmation that Microsoft will not be making prohibited in-kind contributions by offering a package of enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers, including but not limited to federal candidates and national party committees.

BACKGROUND

Russian attempts to interfere with elections in the United States and around the world have been widely reported on, and U.S. intelligence officials predict such efforts will continue during this year's congressional elections. *See, e.g.*, Oren Dorell, *Alleged Russian political meddling documented in 27 countries since 2004*, USA TODAY (Sep. 7, 2017), *at* https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/; Matthew Rosenberg, Charlie Savage, and Michael Wines, *Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn*, N.Y. TIMES (Feb. 13, 2018), *at* https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html; Memo. from Cmmr. Ellen L. Weintraub re Rulemaking proposal to combat foreign influence in U.S. elections (May 17, 2018), https://www.fec.gov/resources/cms-content/documents/2018-05_ELW_Rulemaking_Proposal_to_Combat_Foreign_Election_Influence.pdf.

Although much attention has been given to the Russian "Internet Research Agency's" attempts to sow discord through online propaganda targeted at American voters, the hacking of the online accounts of political operatives and party committees also must not be overlooked. *See, e.g.*, Ofc. of the Director of Nat'l Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections" (Jan. 6, 2017) at 2-3, *available at* https://www.dni.gov/files/documents/ICA_2017_01.pdf; Ellen Nakashima, *U.S. Investigators Have Identified Russian Government Hackers Who Breached the DNC,* WASH. POST (Nov. 2, 2017), *available at* https://www.washingtonpost.com/world/national-security/prosecutors-have-identified-russian-government-hackers-who-breached-the-dnc/2017/11/02/f38b9b18-bfd3-11e7-8444-a0d4f04b89eb_story.html?utm_term=.d6d2e3091d3f); *The John Podesta Emails Released by*

WikiLeaks, CBSNEWS.COM (Nov. 3, 2016), *available at* https://www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/.

With more than 60 million users of its paid O365 cloud-based productivity software and unpaid Outlook.com and Hotmail.com web-based e-mail services,[1] Microsoft is in a unique position to protect election-sensitive users of its products against such hacking. To that end, as part of its "AccountGuard" initiative, Microsoft plans to provide a package of enhanced online account security protections for election-sensitive users of its O365, Outlook.com, and Hotmail.com products at no additional cost.

These account security protections will be offered to "election-sensitive customers" in a phased approach and on a nonpartisan basis, beginning with:

- Federal, state, and local candidate committees;
- National and state political party committees;
- Campaign technology vendors; and
- Think tanks and democracy advocacy non-profits.

After a successful pilot, Microsoft may expand the package of enhanced account security protections to state and local election administrators as well as journalists and other 501(c)(3) non-profit entities. The package also may be offered to 501(c)(4) advocacy groups and other at-risk user groups engaged in election-related advocacy.[2]

In order to receive the enhanced security protections, election-sensitive customers will need to opt into the program and provide certain information about their online accounts and assets that will enable Microsoft to identify those accounts and assets and notify participating election-sensitive customers of security threats and breaches. The enhanced security protections will consist primarily of:

(1) Prescriptive Guidance, Documentation, and Trainings – Participants in the AccountGuard program will receive access to documentation, webinars, and possibly in-person cybersecurity trainings tailored to the specific needs of the campaign community.

(2) Nation State Notifications Across Accounts – Microsoft has a threat intelligence division that tracks individual, organizational, and governmental hackers around the world who are actively attempting to or who may soon interfere with customers' use of Microsoft products or breach Microsoft's systems.

---

[1] Microsoft makes a profit from its unpaid Outlook.com and Hotmail.com products by selling advertising within these products. Because these products are available at no-cost to any user, they do not result in an in-kind contribution to political committees that use these products. *See* AO 2004-6 (Meetup).

[2] This advisory opinion request uses the term "election-sensitive customers" or "election-sensitive users" hereinafter to refer to all of the types of entities and persons enumerated above.

As part of the AccountGuard service, Microsoft will utilize the results of the threat intelligence team's research to investigate, confirm, and notify AccountGuard customers if their O365, Outlook.com, or Hotmail.com accounts have been targeted or breached by a known nation-state actor.

(3) Remediation Recommendations – Microsoft proposes to provide election-sensitive customers of its O365, Outlook.com, and Hotmail.com products who opt into the AccountGuard service with e-mail and telephone technical support, at no additional cost, to assist them in creating a secure online environment as well as to create custom remediation recommendations should their account be breached.

Microsoft currently includes some level of personal telephone and email technical support for nearly every customer of almost all of its products. This basic technical support includes assistance with unauthorized account access for unpaid individual and paid business e-mail accounts. Microsoft offers a higher level of Premier Support for business customers at a per-hour cost. In addition, Microsoft's Enterprise Cybersecurity Group provides more extensive incident response and remediation services to its paid business customers for an additional fee. Microsoft occasionally waives the fee for its Enterprise Cybersecurity Group's services for certain high-priority customers.

The hands-on technical support that Microsoft proposes to provide to its election-sensitive customers under the AccountGuard service would be similar to, although not as extensive as, the cybersecurity assistance provided through its Premier Support and Enterprise Cybersecurity Group.

Aside from the public benefits of the AccountGuard service, Microsoft has strong business considerations for implementing this program. Specifically, election-sensitive entities and organizations are often customers of Microsoft's products, and Microsoft believes making the AccountGuard security protections available to them at no additional cost will help Microsoft maintain and increase market share among those customers.[3] Microsoft also recognizes that its election-sensitive customers are generally not-for-profit entities, and therefore have relatively fewer resources to spend on cybersecurity than do Microsoft's for-profit customers.

[3] Microsoft may wish to eventually expand its AccountGuard program to include partnering companies, such as Facebook, Twitter, etc., although there are no agreements with such companies at this time. (These companies' products generally do not compete directly with Microsoft's products.) Under such an alliance, Microsoft envisions that participating companies would collaborate on providing election-sensitive customers with a package of online account security protections, including those described above and similar security tools. An election-sensitive customer that has online accounts with each participating company would be able to register and opt into the program on one website, and would receive the security protections for the accounts that the customer has with each participating company.

In addition, Microsoft anticipates receiving data about online security threats from the accounts of participating election-sensitive customers that will be highly valuable to Microsoft's efforts to enhance the cybersecurity of all of its products. This threat intelligence is of such value to Microsoft's product development that Microsoft occasionally purchases this type of data and related security information from other companies.

Moreover, Microsoft has a compelling business interest in maintaining its brand reputation. As evidenced by the continued public focus on Russian efforts to influence the 2016 U.S. elections, Microsoft's corporate reputation could sustain severe and long-term damage if hackers were to compromise the integrity of upcoming and future elections by breaching election-sensitive customers' Microsoft accounts.

The proposed package of online account security protections for election-sensitive customers also is consistent with Microsoft's ordinary course of business and existing marketing practices. Specifically, Microsoft currently differentiates the O365 packages and pricing it offers to different types of users, including public-sector entities, educational institutions, teachers and students, small and large businesses, start-up companies, and 501(c)(3) non-profit organizations. *See, e.g.*, Microsoft Office, *at* https://products.office.com/en-us/home; Microsoft Education, *at* https://www.microsoft.com/en-us/education/products/windows/shapethefuture.aspx; Microsoft for Startups, *at* https://startups.microsoft.com/en-us/; Compare Office 365 Nonprofit Plans, *at* https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing?tab=1. Microsoft also routinely offers free workshops and trainings, including cybersecurity trainings, that are tailored to different types of customers. *See, e.g.*, Microsoft Events, *at* https://www.microsoft.com/en-us/store/locations/events; Microsoft MTC MISO Workshop, *at*https://www.microsoftevents.com/profile/form/index.cfm?PKformID=0x3987189abcd.

QUESTION PRESENTED

Microsoft seeks confirmation that it will not be making prohibited in-kind contributions by offering a package of enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers, including but not limited to federal candidates and national party committees, as described above.

DISCUSSION

Corporations are generally prohibited from making contributions, including in-kind contributions, in connection with a federal election. 52 U.S.C. § 30118. An in-kind contribution generally includes "the provision of any goods or services without charge or at a charge that is less than the usual and normal charge for such goods or services." 11 C.F.R. § 100.52(d)(1).

Nonetheless, the Commission has concluded that a vendor "may charge different fees to political committee clients than it charges to non-political clients" without making an in-kind

contribution, so long as "any variation in fees will be based on business considerations and will not be based on political considerations." AO 2018-05 (CaringCent).

Accordingly, the Commission has determined that AT&T's proposal to charge political committees "substantially less" to process contributions made by text message (SMS) than what the company typically charges to process SMS payments to commercial vendors would not result in an in-kind contribution from AT&T. AO 2012-31 (AT&T). The Commission concluded the lower fee for political committees was based on "commercial considerations, including the volume of transactions that AT&T expects to process, the dollar amounts of those transactions, the volume of work that the transactions will generate for AT&T's call centers, and the protection of AT&T's brand and relationship with its wireless customers. The rate structure, moreover, will be set to ensure that AT&T recovers its costs and receives a return." *Id.*

Relatedly, the Commission has determined that Bell Atlantic's proposal to provide "national campaign coordinators" to assist presidential campaigns with arranging telephone service at no additional charge would not result in an in-kind contribution from AT&T or other participating telephone companies. AO 1987-27 (Bell Atlantic). Although the Commission noted the functions of the "national campaign coordinators" were "clearly 'services' of value to a presidential campaign," it nonetheless concluded the proposal was permissible because "Bell Atlantic will be adequately compensated for these services." *Id.*

In addition, the Commission has permitted a bank to waive certain service fees and costs charged to political committees where the waivers are "within the context of a pre-existing business relationship and using the same considerations it uses with all of its clients," and "is part of the Bank's practice in the normal course of business regarding its commercial customers and is normal industry practice." AO 1994-10 (Franklin National Bank).

Here, Microsoft's proposal to provide enhanced online account security protections at no additional charge on a nonpartisan basis to election-sensitive customers is based on business and commercial considerations and not political considerations. As explained above, Microsoft believes its AccountGuard service will help maintain and expand its market share among election-sensitive customers, assist in the company's product development through the threat intelligence gained from participants in the program, and protect the company's brand reputation by reducing the risk that election-sensitive customers' Microsoft accounts are compromised.[4] These are similar to the business and commercial considerations the

[4] Protecting a company's brand and customer relationships, which the Commission has concluded is a permissible reason for providing preferential pricing to political committee customers, is distinguishable from generating "publicity," public "goodwill," and "promotional value," all of which the Commission has concluded are not permissible bases for providing free goods and services to political committees. *Compare* AO 2012-31 (AT&T) *with* AOs 1996-2 (CompuServe) and 1991-23 (Nat'l Assoc. of Retail Druggists).

Commission determined were permissible reasons for vendors to provide preferential pricing to political committee customers in AOs 2012-31 (AT&T) and 2018-05 (CaringCent).

Also as explained above, Microsoft's proposal is consistent with its normal course of business of providing different O365 packages at different prices to different types of users, providing its Enterprise Cybersecurity Group's technical support services at no additional cost for certain high-priority customers, directing its threat intelligence division to track security threats against certain high-profile customers' online accounts, and providing free workshops and trainings (including cybersecurity trainings) that are tailored to different types of customers. *See* AO 1994-10 (Franklin National Bank).

Microsoft's proposal also is consistent with normal industry practice. Technology companies realize they have a social responsibility and compelling business considerations for protecting their products from being misused by malicious foreign interests seeking to influence elections in the U.S. and around the world. To that end, Facebook, Twitter, and Google have all recently implemented additional screening and transparency measures for purchasers of political ads on their platforms. *See* Facebook, Political Advertising, *at* https://www.facebook.com/policies/ads/restricted_content/political; Twitter, Political Campaigning, *at* https://business.twitter.com/en/help/ads-policies/restricted-content-policies/political-campaigning.html; Google, U.S. election ads verification, *at* https://support.google.com/adwordspolicy/contact/us_election_ads. Google's Jigsaw division also recently promoted a free service known as "Project Shield" to candidates, campaign committees, section 527 political organizations, and political committees to protect against distributed denial of service ("DDoS") attacks. *See* Dan Keyserling, Extending Free DDoS Protection for U.S. Political Organizations, *at* https://medium.com/jigsaw/extending-free-ddos-protection-for-u-s-political-organizations-94ef1bb896f.

While Microsoft cannot predict or calculate at this time whether the security protections offered through its AccountGuard service will result in a direct economic profit from each and every participating election-sensitive customer, for the reasons discussed above, Microsoft believes the program will be profitable to the company as a whole and to its product sales.[5]

More fundamentally, the security protections are being offered for valid business reasons and on a nonpartisan basis to existing and future Microsoft customers, and not "for the purpose of influencing any election for Federal office." *See* 52 U.S.C. § 30101(8)(A)(i). To the contrary, the proposed program will prevent external actors from influencing elections by hacking the online accounts of Microsoft's election-sensitive customers.

[5] We also note that, according to Facebook CEO Mark Zuckerberg, the company is "essentially going to be losing money on running political ads" for the next few years because of its new vetting procedures for such ads. Peter Kafka, *Facebook will spend so much reviewing political ads this year that it will lose money on them*, RECODE.NET (May 1, 2018), *at* https://www.recode.net/2018/5/1/17309514/facebook-money-politics-advertising-2018-mark-zuckerberg.

The AccountGuard service also is distinguishable from the free items the Commission has concluded are impermissible for a corporation to provide to a political committee with whom the corporation otherwise would have no "business relationship." *See* AOs 1996-2 (CompuServe) and 1991-23 (Nat'l Assoc. of Retail Druggists); *see also* AO 2012-26 (m-Qube) (explaining AO 1991-23). In AO 1996-2 (CompuServe), the requester proposed to waive its monthly subscription fee for its main service for political committees with whom the requester otherwise had no business relationship. Similarly, in AO 1991-23 (Nat'l Assoc. of Retail Druggists), the requester proposed to have a company donate an item to a political committee as a prize for the committee's fundraising raffle where the company otherwise had no business relationship with the committee. By contrast, Microsoft has or will have a business relationship with each and every election-sensitive customer that opts into its AccountGuard online account security protections, whether as a paid subscriber of an O365 product or as an unpaid user of Outlook.com or Hotmail.com. Therefore, the conclusions in AOs 1996-2 (CompuServe) and 1991-23 (Nat'l Assoc. of Retail Druggists) do not apply to Microsoft's proposal.

CONCLUSION

For the reasons discussed above, the Commission should confirm that Microsoft will not be making prohibited in-kind contributions by offering a package of enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers, including but not limited to federal candidates and national party committees.

Please do not hesitate to contact us should you have any questions regarding this request.

Sincerely,

Jan Witold Baran
Eric Wang

cc: Chair Caroline C. Hunter
Vice-Chair Ellen L. Weintraub
Commissioner Matthew S. Petersen
Commissioner Steven T. Walther