

RESPONDENT'S COMPLAINT #4 BRIEF

RESPONDENT has not committed any violations of university policy.

COMPLAINANT has again asked the Commission to award them an election not on the basis of votes, but points—entertaining a tradition of legal survivor where elections are decided by less than a dozen people and not the students of Indiana University. In this brief, which is divided into a formal reply and then concise answers to the Commission's questions, we aim to dispel the serious but unsupported and misguided allegations by COMPLAINANT.

Please note, out of significant deference to this process, we have decided to suspend use of campaign emailing, including that of all opt-in contacts, until this can be further adjudicated. RESPONDENT has not used or contacted a university address through DirectIQ since Monday April 6, 2020. RESPONDENT does not see emailing as a central part of its campaign strategy and has used it sparingly. Indeed, the engagement we receive from person to person meetings, endorsements, earned media, peer-to-peer texting, SMS marketing, and, most crucial, social media marketing significantly surpasses that of email.¹ Following the certification of elections, we intend to destroy all campaign data so that it may not be repurposed.

¹ In example, during the short course of the campaign, we have seen 100,000s of impressions on Instagram alone. This is further complemented by extensive social media advertising which generates many multiples of our organic traffic. **We have not sent any campaign email to or with a university account in the 10 days leading up to the election, perhaps the most critical timeline for campaign activities.** We expect to need only 1,750 votes to win in a competitive IUSG election and believe that we can and will do so by a substantial margin without the use of email marketing.

REPLY TO COMPLAINT

In Complaint #4, COMPLAINANT asserts that RESPONDENT has violated the IUSG Election Code (“the Code”) and by incorporation university policy by campaign members obtaining, using, and contacting university email addresses. Further, it suggests, though never formally complains, that RESPONDENT has used IUSG resources for its campaign. RESPONDENT has not violated university policy and has not used any IUSG resources for its campaign.

I. COMPLAINANT has not made a claim that can be addressed by the Commission and therefore the Commission cannot grant relief.

The Code sets out specific procedural considerations which all parties must abide by to ensure fair, transparent, and efficient outcomes. COMPLAINANT fails to meet this bar in three ways: (a) no claims were timely filed, (b) violations of university policy must be adjudicated by a student conduct process, and (c) COMPLAINANT has not articulated by clear and convincing evidence any violation of the Code.

a. Timeline—Defy has failed to file a complaint related to the acquisition or use of email or other data within 48 hours of the action.

Second 704 of the Code states, “Complaints may only be issued about a violation that has occurred within the last 48 hours. If it has been more than 48 hours since the violation occurred, tickets or candidates may not file a complaint about that violation.” Defy’s complaint was filed on April 12, 2020 but all of the alleged acts for which their complaint rest on took place April 6, 2020 and before.² Indeed, the only potentially meritable complaint is not about improper use of data but (1) whether such data is properly accounted for on financial statements and (2) whether the alleged retention alone, within

² This is the date of the last use of DirectIQ for email marketing purposes by RESPONDENT.

48 hours of the complaint, of that data is a violation of university policy. The first question is not raised by COMPLAINANT and may be set aside. This leaves only considerations of whether holding student data within 48 hours of the COMPLAINT is a violation of the Code (and incorporated by reference university policy) and not whether obtaining or using data is a violation. None of the allegations provided appear to reach this question either.

Further, even if the filing of a financial statement were to trigger such considerations about data retention and university policy, COMPLAINTANT failed to do so within the allotted 48-hour window, as well. Even when defined by COMPLAINTANT's timeline window, which closed at 12 AM Thursday April 12, 2020, the COMPLAINT appears to have been filed after this time. Assuming their complaint was filed at 12:00:01 AM EST Thursday April 12, 2020 or later, which the Election Commission is in a position to confirm, the complaint was not timely filed and no relief can be granted by the Commission. Moreover, the more accurate window of a timely filing is 48 hours from the time of submission or 48 hours within the time of publication by the Commission. The COMPLAINT was seemingly not filed within either period and therefore no violations can be addressed.

While a strict rule, this provision of the code was put in place to guard against late allegations and to ensure efficient election processes, among other reasons. To allow COMPLAINTANT to bring in potential violations beyond this period would be an infidelity to the text of the Code and its purpose. The Commission, notably, has held up this strict timeline in previous years, including in its ruling on Complaint #2 of the 2019 Executive Election.³ This same analysis should be applied to COMPLAINTANT's allegations, where a

³ 2019 – Complaint #2 (“The timeline of the incident is unclear, as the text messages would have taken place within 48 hours from when the complaint was submitted but not the event referred to in the messages.”)

record of an act cannot incorporate the act itself into the 48-hour window. The COMPLAINT must be filed within 48 hours of the act itself.

b. University Adjudication—A violation of university policy must be determined by the proper adjudicatory body of the university.

The violation of a university policy, as alleged here, may only be determined through a student conduct process where a participant's rights are preserved. It should not be determined by the ad hoc findings of an administrator or by the Commission itself. We would readily submit these questions as individuals to any conduct proceeding if ever warranted and pursued. At this time, however, we see no basis for a conduct proceeding and are aware of no proceeding taking place. To provide otherwise would allow for arbitrary and inaccurate interpretations of university policy and also deny participants the substantive and procedural protections of a university conduct process, including the opportunity to obtain counsel.

The more appropriate approach, and the one contemplated by Section 508 of the Code, would be to file a complaint within 48 hours of a violation being found by the university.

c. Abuse of Office—Complaint #4 suggests RESPONDENT used IUSG resources in its email marketing, but has not cited to Section 503 of the Code or made a formal complaint to this end.

We can confirm that IUSG Congress does not have access to university mailing lists and therefore no members of our campaign could have access to this information through IUSG. **See Exhibit 1.** Even if the campaign had done so—which it did not and never would do as it is a gross ethical violation of our respective roles—the act would have occurred well outside of the 48 hours timeline necessary for filing a complaint and no complaint on this matter has been articulated.

d. Sufficiency of the evidence—Defy’s complaint relies on conjecture and does not provide clear and convincing evidence of any misconduct.

Ultimately, the burden falls on the COMPLAINANT to show by clear and convincing evidence a violation of university policy. Clear and convincing evidence means “that evidence must be highly and substantially more likely to be true than not.”

COMPLAINANT has not met that bar. In none of its allegations has COMPLAINANT provided sufficient evidence of a violation but has instead asked the Commission to buy into nothing more than suspicion and subjective interpretations of university policy undergirded by three entries of evidence: (1) a financial statement, (2) a screenshot of an email, and (3) a screenshot of the same email to another recipient. Clear and convincing evidence demands more of COMPLAINANT for each of the allegations it has made.

II. The actions described by COMPLAINANT are not violations of university policy.

While not addressable by the Commission under procedural grounds, *supra* Part I, RESPONDENT rebuts all allegations of violations of university policy and addresses each provided by COMPLAINANT.

a. Use of Electronic Mail IT-21

COMPLAINANT cites two relevant lines from IT-21: (1) *“Electronic mail will not be sent by members of the University community to persons with whom the sender does not have an established mutually-accepted personal, business, or academic relationship”*; and (2) *“University electronic mail will not be used for personal commercial purposes or for personal financial or other gain.”*

The use of electronic mail for First Amendment protected purposes (i.e., political speech) is not a commercial activity and does not otherwise constitute personal or financial

gain. COMPLAINANT fails to provide any reasoning, despite its burden in doing so, on how a violation has occurred. Yet, university policy does not and cannot supersede federal law and longstanding jurisprudence on protected political speech.⁴ If COMPLAINANT's

⁴ See e.g., *Candid answers to CAN-SPAM questions*, U.S. Federal Trade Commission (Aug. 18, 2015) ("The CAN-SPAM Act applies only to commercial email, whether sent individually or in bulk. It doesn't apply to non-commercial bulk email. Furthermore, political messages are protected under the First Amendment. Of course, many groups not covered under the law have chosen voluntarily to honor UNSUBSCRIBE requests. But if you're getting unwanted email from entities not subject to CAN-SPAM that don't offer an UNSUBSCRIBE feature, another option is to contact them directly to express your preference not to receive more messages. (Don't just respond to the email, which may not be read.) If any group is trying to win you over – whether it's an advertiser, an advocacy group, a candidate, etc. – it could be persuasive to let them know how you feel.").

See e.g., FIRE'S GUIDE TO FREE SPEECH ON CAMPUS — FULL TEXT, <https://www.thefire.org/research/publications/fire-guides/fires-guide-to-free-speech-on-campus-3/fires-guide-to-free-speech-on-campus-full-text-2/>

The University of Oklahoma, informed students and faculty via email a few months before 2008 election that "[a]s a state agency ... the University may not endorse or oppose a particular candidate for office," and that this prohibition "includes the use by its faculty, staff and students of its email and network systems." The announcement further stipulated that the university's email and network systems could not be used to send messages endorsing or opposing a candidate, or even for forwarding "political humor/commentary." The university's (erroneous) rationale was that such discussion placed the school at risk of losing its tax exemption.

This is a classic example of an overbroad ban on core political speech protected by the First Amendment. The school was banning speech protected by the First Amendment. **The Internal Revenue Service has made clear that, in the campus context, the restriction on political activity placed on non-profit, tax-exempt entities is interpreted differently in light of the educational mission of colleges and universities, allowing certain activities (such as a political science class that requires students to work on a campaign, as long as the student, not the instructor, is allowed to choose the campaign, or political editorials in favor of candidates in a student newspaper) that would otherwise likely constitute prohibited activity for tax-exempt entities.** Restrictions on political activity apply to the institution itself and those reasonably perceived to be speaking on its behalf, not to individual students, faculty, or staff engaged in clearly individual, unaffiliated activity.

The University of Oklahoma recognized the error of its ban on political speech. In a follow-up email, a university official stated, "The policy has been clarified to those who have raised questions. I felt that in addition it should be clarified to the entire university community...Individual free speech by all members of the university community is fully protected. The earlier [policy] was intended to remind all of us that no one should presume to speak on behalf of the university in a way that would imply that the university, as an institution, is supporting a political candidate, party or cause. This, however, does not limit the right of anyone to express individual views."

At Michigan State University ("MSU"), a student government leader was charged with violating MSU policy for sending out an email to around 400 faculty members. Specifically, the student was charged with violating MSU's "Network Acceptable Use Policy" and other provisions, including the university's policy prohibiting the use of university equipment for an unauthorized purpose. Following an investigation, university

standard were applied, students' expression would be censored and COMPLAINANT too would almost certainly have violated university policy. **See Exhibits 2-3.** Even if COMPLAINANT has used a private email address in its own mailings it is certainly communicating about political purposes, as they would describe as for its own private gain, to university email addresses. RESPONDENT has not filed a complaint on this matter because we believe this is a dangerous and inaccurate account of university policy. University policy here is directed to stop the distribution of commercial spam not to suppress student expression.

b. IU Acceptable Use Agreements

While COMPLAINANT has not articulated reasons why RESPONDENT has violated the Acceptable Use Agreements, which is their burden to prove by clear and convincing evidence, we will address each prong:

1. *Access institutional information only in the conduct of university business and in ways consistent with furthering the university's mission of education, research, and public service.*

The use of university email services for promoting a student government election falls within this definition, just as the use and creation of university email addresses such as iudems@indiana.edu does. University resources are regularly used for political activities by students and can be done so long as the university itself or its representatives are not engaging in

administrators argued that the student's email was the electronic equivalent of junk mail and disrupted the activities of its recipients. The student was found guilty of "spamming" following a hearing, and a disciplinary warning was placed in her file. Joined by 12 national civil liberties organizations, the Foundation for Individual Rights in Education wrote MSU an open letter protesting the student's punishment, noting MSU's "anti-spam" policy is constitutionally suspect on its face. It is vague and allows the university unfettered discretion, requiring prior administrative approval before sending e-mails to more than approximately "20-30" recipients. It also discriminates on the basis of content, prohibiting e-mail sent "for personal purposes, advertising or solicitations, or political statements or purposes." Because of this, the university dropped all charges against the student.

political speech. The university cannot bar the use of its resources for student expression—student expression and civic participation is, after all, part of the university’s core mission.

2. *Use only the information needed to perform assigned or authorized university duties.*

This language is inapplicable as authorization includes the use of email for promoting student activities and expression. The university cannot create prior restraints on student expression.

3. *Never access any institutional information to satisfy your personal curiosity.*

This data was not used for the satisfaction of a personal curiosity and is public-institutional data, at most, that the university places “little or no restrictions” on.

4. *Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.*

See supra a.

5. *Never disclose University-internal, Restricted, or Critical data (as defined by policy; see above) or distribute such data to a third party in any medium (including oral, paper, or electronic) without proper approval, and in the case of Restricted or Critical data, without a contract processed through or waived by the IU Purchasing Department.*

This is public data and does not meet any of the above definitions.

6. *Never send mass email (i.e. unsolicited bulk email or spam) without appropriate approval.*

COMPLAINANT does not send UBE, which applies to commercial speech, and does not need prior authorization for First Amendment protected speech—this would be an impermissible form of prior restraint and allow for content-based regulation of political speech.

Finally, COMPLAINANT notes, seemingly without point or in hopes that someone else can color in their outline, that an IU Acceptable Use Agreement states examples of relevant federal laws including FERPA and the Indiana APRA, neither of which are applicable here. FERPA handles student record data and excepts the disclosure of Directory Information, including names and email addresses. Indiana APRA similarly allows for the disclosure of this information, which the

university willingly does through its public-facing directory and other mediums. No violation has occurred.

c. Management of Institutional Data DM-0

COMPLAINANT cites in relevant part the following university policies, though never articulates how RESPONDENT has violated these other than to conclude that RESPONDENT has:

Users of institutional data must:

- *Access data only in their conduct of university business, and in ways consistent with furthering the university's mission of education, research, and public service.*

Previously addressed.

- *Respect the confidentiality and privacy of individuals whose records they may access.*

This is public information. No confidential or sensitive information is stored or has been received by RESPONDENT.

- *Observe any ethical restrictions that apply to the data to which they have access.*

There are no restrictions at play here. This is not research data, PHI, etc.

- *Abide by applicable laws, regulations, standards, and policies with respect to access, use, disclosure, retention, and/or disposal of information.*

Previously addressed.

Users of institutional data must not:

- *Disclose data to others except as required by their job responsibilities.*

RESPONDENT has not disclosed data to any party (even our vendor does not have physical access to the data) although it is public information and can be redisclosed without issue.

- *Use data for their own or others' personal gain or profit.*

Previously addressed.

- *Access data to satisfy personal curiosity.*

Previously addressed.

- *Institutional Data falls into four classifications (Critical, Restricted, University-Internal & Public). In the absence of being formally classified, institutional data should be treated as University-Internal by default.*

The university classifies names and email data as public and provides it in a public facing directory.

Additionally, the Management of Institutional Data policy states consequences for violation: "Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these."

Finally, it appears COMPLAINANT cites to irrelevant language to seemingly intimidate or harass RESPONDENT. These penalties may only be assessed by the university following a conduct process.

d. Use of Electronic Mail IT-21

Here, COMPLAINANT again concludes, without evidence or reasoning, for which the burden is theirs alone, that "The Inspire campaign violated following [sic] 'Use of Electronic Mail' policies."

We address each on its merits:

1. Electronic mail will not be sent by members of the University community to persons with whom the sender does not have an established mutually accepted personal, business, or academic relationship.

As student government officials individually and as a campaign for student government, we have an accepted relationship with all students. This is, however, not required for First Amendment protected speech but for commercial or otherwise non-protected speech and the university policy is inapplicable in this instance.

2. Sensitive institutional and personal information will not be sent via email, unless specific steps are taken to confirm that the transmission is secure.

This is not sensitive and personal information such as PHI, student records, etc.

3. University electronic mail will not be used for personal commercial purposes or for personal financial or other gain.

Previously addressed.

4. Mailing lists will be moderated so that inappropriate postings are intercepted and rejected, and electronic mailing lists will be protected as far as technically possible from commercial exploitation.

This is a statement of university practice and not an articulation of a violation.

e. Appropriate Use of Technology Resources IT-01

COMPLAINANT again concludes a violation but provides insufficient evidence of or reasoning to meet a clear and convincing standard. We address each of the allegations on their merits:

“Unless otherwise specified in this policy or other university policies, use of Indiana University information technology resources is restricted to purposes related to the university's mission of research and creative activity, teaching and learning, and civic engagement. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, official business with the university, and other university-sanctioned activities. Individuals may not share with or transfer to others their university accounts including network IDs, passwords, or other access codes that allow them to gain access to university information technology resources.”

This policy is applicable to individuals sharing their access information for university resources, not groups contacting individuals.

“Indiana University technology resources may not be used in a manner that violates the law, for private commercial activities (defined below) that are not approved by the university, for personal private gain, or for political campaigning and similar activities that are inconsistent with the university's tax-exempt status.”

Resources were not used in a manner that violated the law, for private commercial activities, or for personal private gain. While potentially political campaigning—though by no means political in the conventional sense of aiming to set policy for a decision making body—the university cannot restrict students from using its resources for First Amendment protected activities.⁵

Indeed, similar policies at Big Ten Schools have been successfully challenged in Court because they are unconstitutional. A more accurate reading of this is the restriction of political campaigning on behalf of the university or by its administrators in a way that would jeopardize its tax-exempt status. This is why organizations like the College Democrats have an official @indiana.edu email address, why IUSA/IUSG campaigns for years have used email marketing to

⁵ See supra.

promote their candidacies to students, why students can send and receive political messages, etc. The university does not and cannot restrain student political expression. This policy simply restricts individuals from speaking on the university's behalf for political purposes.

f. Disclosing Institutional Information to Third Parties

COMPLAINANT again provides a conclusion without sufficient evidence or reasoning to reach a clear and convincing standard. We address each part on its merits:

Indiana University's 'Disclosing Institutional Information to Third Parties' policy describes the procedures agents of the university must abide by when disclosing university institutional information to a third party. This party must be "aware of and take proactive steps to reduce the risks associated with the sharing of information."

This is public data and is already disclosed by the university. It may be readily re-disclosed for any lawful purpose. That said, we follow industry customs for use of the data as we don't want it to be used for non-campaign purposes. See Questions Section.

Additionally, the policy states: "The university also recognizes the need to share institutional information with partners to accomplish its mission and that, when disclosing this information, the university must exercise due care. Furthermore, to ensure compliance with applicable federal and state laws, regulations, and university policies, it is vital to evaluate and approve the ability of third parties to appropriately handle and protect information before information is shared."

No federal or state law is implicated nor has COMPLAINANT made an argument for a violation.

Under the definition of Disclosing Information, the policy also reads: "Maintenance of information: examples include warehousing paper or electronic records at a third party site; using a hosted platform provider to store institutional information; email outsourcing;"

This if for the maintenance of information, a topic COMPLAINANT has not alleged a violation. Applicable practices for destroying data, etc. have been and will be followed.

Furthermore, procedures in place moving forward with approving of third-party disclosures include: Prior to disclosing institutional information, the agent is responsible for initiating and managing the process below to ensure that:

- *There is an adequate understanding of the third party's security environment;*
- *Business needs, risks, and mitigating safeguards are analyzed and documented; and*

- *Institutional information is adequately protected*

This is public data and these guidelines therefore do not apply. Nonetheless, the information provided is sufficiently secured. See Questions Section.

III. COMPLAINANT's allegations all implicate First Amendment exemptions as emails were sent for the purpose of student government elections and social issues pertinent to campus—not commercial purposes.

University students may freely use university emails and other technology to promote political causes. This principle is echoed in decades of First Amendment caselaw and a markedly similar policy was removed just this March at the University of Iowa because of its impermissible content-based restriction on political speech.⁶ Indiana University's policy may only be read to restrict employees (i.e., faculty and staff) from using resources to promote political causes on the university's behalf. We, however, are not asking in the capacity of either when distributing emails.

IV. If the Commission were to find for COMPLAINANT, the appropriate remedy is a 4-point penalty against RESPONDENT.

As we have addressed in our replies to COMPLAINANT's repeat attempts to disqualify RESPONDENT, elections should be won on the basis of votes and not points. The Code provides upwards of a 6-point deduction against any violator, though we would counsel that if any violation were to have occurred it was done out of ignorance or negligence and not malice.

Emailing is but a small part of our campaign and a means we have used only sparingly. This is largely because we can achieve a much greater engagement rate from

⁶ Tyler Davis, *Free-speech nonprofit drops lawsuit vs. Iowa State after school adjusts chalking, email policy*, Des Moines Register (Mar. 13, 2020) <https://www.desmoinesregister.com/story/news/crime-and-courts/2020/03/13/free-speech-lawsuit-against-iowa-state-dropped-university-adjusts-policies/5042712002/>

social media marketing and other forms of campaigning undertaken by both campaigns. In example, a targeted \$250 investment (i.e., the cost of email marketing) through Facebook / Instagram advertising would be expected to have approximately 40,000 – 100,000 impressions, far surpassing not only the reach but recall lift of an email campaign. While a welcome tool, it is just one of many in the chest.

Out of an abundance of caution and deference to the Commission's process, RESPONDENT has discontinued collecting or using university email addresses entirely and has sought a refund for services not rendered by DirectIQ so it may be reallocated toward other campaign activities. We will, of course, submit any reimbursement received to the Commission in our final financial statement.

After a complete process, should the Commission find a violation, the Commission should in light of these many factors institute the proscribed 4-point penalty against RESPONDENT. The acts described are insufficient for severe penalties or disqualification.

ANSWERS TO THE COMMISSION

1. How were student emails collected and how many were collected?

Contact information is and was collected from a variety of sources including from volunteers who provided personal contacts, opt-ins from digital marketing, opt-ins from our website, opt-ins from other landing pages, and the use of publicly available data.⁷ Notably, all non-opt-in data was collected before the campaign began, before our candidates had decided to run, or before a leadership team was created. Moreover, the Inspire campaign, along with Defy, could easily access most full-time student emails through Zoom today, for example, using the company contacts section.⁸ We have not purchased email contacts from a vendor and do not have access to Salesforce or other university data which would allow organizations like IUSG or campaigns to generate an all-encompassing, clean, targeted campus email list.

For all contacts (emails, SMS, Messenger) we have used segmented lists of approximately 45,000 – 50,000 unique students, faculty, media, and other parties.

a. Was an IUSG resource used in collecting these email addresses?

No. IUSG Congress does NOT have access to university mailing resources through Salesforce, Canvas, or other enterprise technology. **See Exhibit 1.** IUSG Congress only obtained its own dedicated Outlook account just this academic year and has received or

⁷ This includes data from the IU Directory (which is publicly available), data obtained using web crawlers, and data pulled from campaign members' personal email contacts and accounts. At no time were university resources breached, data given the campaign by outside parties, data purchased, or otherwise unethical acts taken to obtain data.

⁸ The Contacts section of IU Zoom accounts shows approximately 25,000 – 30,000 university email addresses which could be used by either campaign for First Amendment protected purposes.

contacted less than 1,000 email contacts almost all of which (600+) are for the purposes of press relations and given to it by individuals from past work experiences.

We are unaware if the IUSG Executive Branch, which our campaign leadership team is not a part of, has access to a university mailing list—though likely not as we have never seen a message from IUSG to members or students. If this is the case, we can attest we have not received any data from IUSG. Inspire campaign leadership has never used their respective offices and any data stemming from them to promote their campaign.⁹

2. How many times has this list been used for campaign activities?

This is not one list but several segmented lists according to certain basic demographics (e.g., faculty, media, students) and other factors (e.g., psychographics based on digital marketing, engagements with certain landing pages). Thus far, we have used DirectIQ for the sole purposes of (1) a limited announcement of our campaign, (2) contacting select faculty to raise awareness of elections generally, (3) sharing general information about a COVID-19 townhall during the first week of remote classes, and (4) sharing a petition as individuals to garner support for tuition refunds.

We have received overwhelmingly positive responses from students, faculty, and others contacts with only a handful of disparaging remarks or even requests for being removed (less than 0.05% of all contacts). Indeed, these remarks are almost exclusively

⁹ This is, notably, contrary to the Defy campaign that has, on at least on one occasion, used private IUSG polling data available to it, because of its Presidential candidate's role as a leader of data analytics projects, in its campaign social media. We have opted to not file a complaint on this because it was not brought to our attention until the 48-hour window had passed, a rule we strictly abide by.

from members of the Defy campaign and their acquaintances, including on more than one occasion especially disparaging remarks about our candidates' identities.¹⁰

As required by the code, we have removed all contacts who have requested it well within 36 hours and also removed, at our discretion, any individuals who we otherwise believed violated standards of decency or conduct with which we hope to affiliate our campaign. At no time has the data of other students been exposed to recipients and at no time has a student been able to use a reply-all function to spam other users.

3. What sort of institutional protections were put into place to protect this data?

Our vendor and our campaign submit to industry best practices for data privacy and information security, including dual authentication for the use of certain resources, encryption of data stored in DirectIQ, complex and changing passwords to our accounts, limiting the scope of data to trained and designated individuals,¹¹ cleaning contacts that “bounce” or are nonresponsive, and, notably, committing to destroying all data after the certification of elections so it cannot be breached or disclosed for non-campaign activities. At no time have we ever requested or collected sensitive information (e.g., PHI, academic records, financial data) from contacts. Out of courtesy, we also provide an automatic opt-out option along with a spam complaint function for interested parties at the footer of any communication as is standard practice for the industry.

¹⁰ Including queries such as “which [of our candidates] is more racist” and the use of expletives, threats, and anti-Semitic remarks. Instead of filing complaints we addressed this personally with Defy’s leadership and we welcomed their instructions to members and supporters to stop. This approach also effectively ended likely COMPLAINANT’s repeat attempts to mark our social media accounts as spam, including at one point locking RESPONDENT out of its Instagram account for 5 consecutive days.

¹¹ One has significant work in data privacy as a law clerk for the in-house privacy officer of a major health insurer and the other is a Microsoft intern and is currently working on what the campaign describes as the Student Data Privacy Bill of Rights, a new policy framework to ensure sensitive student data is protected and certain technologies preemptively banned by the university. No other individuals have access to any data and no data kept is sensitive in nature.

4. Were students made aware that their emails were being submitted to a third-party mass emailing service?

Not all recipients are opt-ins and this is not required by law and cannot be by university policy when information is used for First Amendment protected purposes, including the exercise of political speech. We strictly abide by the Code, never allowing for a reply-all scenario and removing all interested parties from all lists within 36 hours of their request. Out of courtesy, we also provide an automatic opt-out option along with a spam complaint function for interested parties at the footer of any communication as is standard practice for the industry.

5. Does DirectIQ retain the user content and thus IU student emails?

No. As it the case with most major vendors, we own the data submitted, it is firewalled exclusively for our use, and this data cannot be shared with other parties for any purpose by any party but authorized members on the account or following a lawful order of a court or similar circumstance. In many states (e.g., Nevada, California, New Jersey) any other practice—especially appropriating customer data—by the vendor would likely be illegal. We restrict this data to only two members of the campaign who have unique experiences in data privacy and information security.

Please note, out of significant deference to this process, we have decided to suspend use of campaign emailing, including that of opt-in contacts, until this can be further adjudicated. We have not sent any email using university accounts or to university accounts since Monday April 6. RESPONDENT does not see emailing as a central part of its campaign strategy and has used it sparingly. Indeed, the engagement we receive from person to person meetings, endorsements, earned media, peer-to-peer texting, and, most

crucial, social media marketing significantly surpasses that of email.¹² Following the certification of elections, we intend to destroy all campaign data so that it cannot be used for impermissible purposes.

¹² In example, during the short course of the campaign, we have seen 100,000s of impressions on Instagram alone. This is further complemented by extensive social media advertising which generates many multiples of our organic traffic.

EXHIBITS

Exhibit 1: Email for Jim Johnson

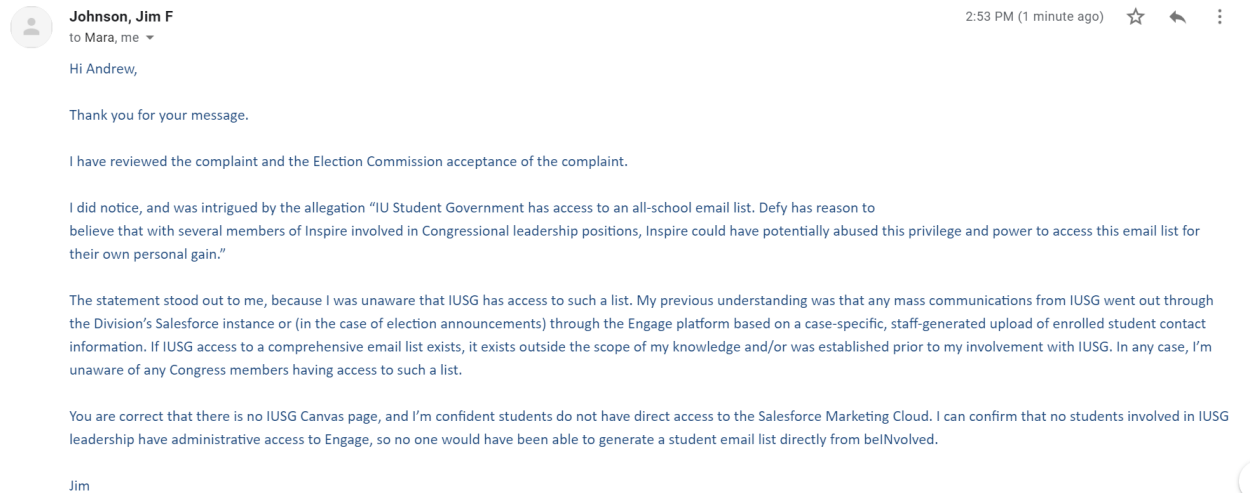


Exhibit 2:

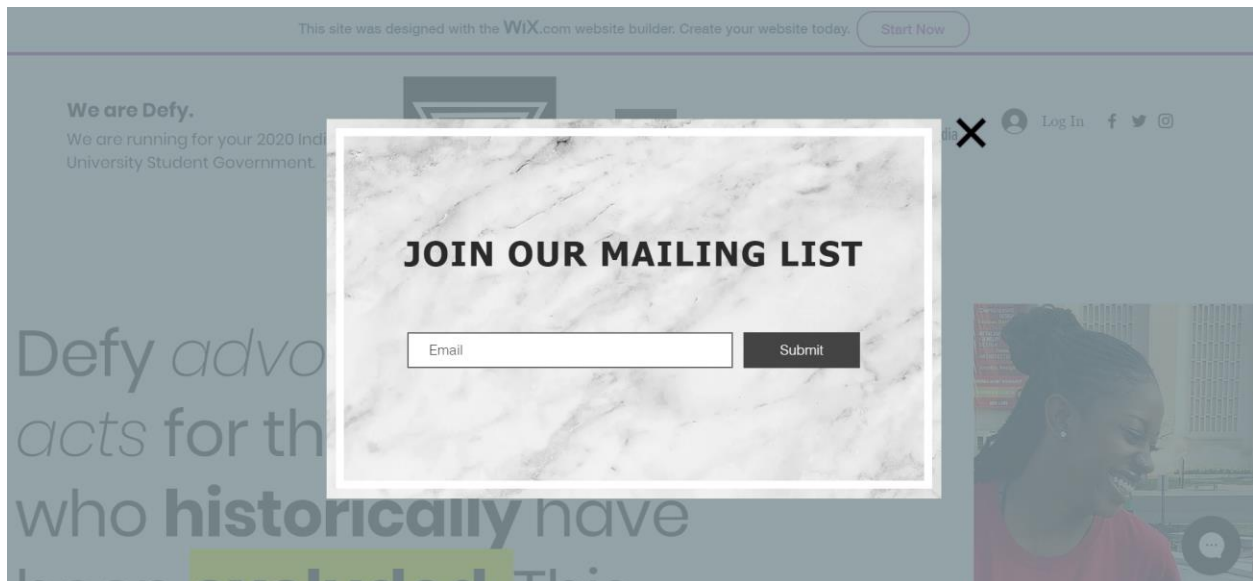


Exhibit 3:

