ELECTRONIC FRONTIER FOUNDATION

November 24, 2021

[redacted]

Dear [redacted],

Re: Buzz Vulnerability Disclosure

We represent Cooper Barry de Nicola, Miles McCain, and Aditya Saligrama (collectively, the students), and are responding to your letter of November 22. The letter demands that, unless the students agree to various terms—including staying silent about vulnerabilities they discovered in the Buzz application and Buzz Media's misleading claims on encryption and user anonymity—within five days including the Thanksgiving holiday, you will "pursue charges."

Your letter comes as a surprise, to say the least. Prior to your involvement, the students provided important information about a critical vulnerability in your software, asking nothing in return. Buzz Media thanked them and acknowledged their report was made in good faith. Perhaps you can appreciate that following up these productive discussions with baseless threats of legal action and even criminal charges leaves a bad taste.

While the students' research might have been embarrassing for Buzz—given that they found fundamental failures to protect user privacy and anonymity despite the app's public claims to do so—their research assuredly did not violate the laws you cite. In the course of their research, the students did not circumvent any effective technical protections on access, nor did they make use of any user accounts that they did not have permission from both Buzz and the account holder to access. Hence, they have not violated the Computer Fraud and Abuse Act or the Digital Millennium Copyright Act. And regardless of whether they violated any applicable Terms of Use, they cannot be held liable for any potential damages resulting from Buzz's own security vulnerabilities.

In addition to its lack of legal merit, your letter is troubling because it violates Rule 3.10 of the California State Bar's Rules of Professional Conduct, which prohibits lawyers from threatening to present criminal charges to obtain an advantage in a civil dispute. While we understand that you dispute the students' right to have conducted their prior security research, the Rule nevertheless prohibits you from conditioning pursuit of criminal charges on their agreement to your demands to resolve that dispute. We expect that you will cease such conduct going forward.

Nevertheless, we would like to have a productive discussion with Buzz, without the artificial urgency of your five-day deadline. As a continuing show of good faith, the students confirm that they do not intend to access the Buzz application again, nor do they retain any user data from Buzz, obviating that aspect of your demands.

As for the demand for confidentiality, in their prior discussions with Buzz, the students affirmatively placed an embargo on talking publicly about this matter until December 8. They will hold to their previous commitment not to speak publicly about their findings until at least December 8, and they are open to further discussions about how users might be notified about the vulnerabilities, among other matters. Rather than creating unnecessary work for all of us during the holiday weekend, we suggest that the parties work out whatever disputes remain on that initial generous timeline.

Finally, please understand that good faith security researchers like the students we represent help build a safer future for all of us who depend on digital technologies. Just as important as discovering security vulnerabilities is reporting the findings so that users can protect themselves and vendors can repair their products. Your legal threats against the students endanger security research, discourage vulnerability reporting, and will ultimately lead to less security. We urge you to reconsider whether this is truly the path Buzz wants to go down. We await your reply and look forward to resolving this productively.

Sincerely,

Andrew Crocker
Senior Staff Attorney

Kurt Opsahl
Deputy Executive Director and
General Counsel

Electronic Frontier Foundation