THE
NEW YORKER
4 TIMES SQUARE
NEW YORK, N.Y. 10036-7441

September 3, 2013

Dear Alexei, Bruce. and team,

We appreciate your thorough research and evaluation of the DeadDrop open-source system initially developed by Aaron Swartz, which *The New Yorker* implemented as Strongbox. It's precisely the kind of audit that we anticipated the open-source nature of the system would invite. We are especially pleased that your tests uncovered no security holes in DeadDrop's core code or in the Strongbox system itself.

We would like to address some of the issues you raised, and your suggestions for making Strongbox even more robust.

Some of the recommendations made by your team – such as loading Strongbox instructions on every page of newyorker.com, to protect potential sources from traffic analysis and hosting the Strongbox page on https – appear practical and we'll begin studying whether and how to implement them. We will also investigate creating a GitHub repository of our most current deployment of Strongbox. Publishing release hashes in the printed magazine is an intriguing idea as well. We have, as you know, consulted with security experts, and we will examine with them the possibility of making our website itself a Tor entry node.

A couple of elements of Strongbox your team questioned were, however, the result of deliberate choices on our part aimed at making the system more secure. For instance, while recognizing the possibility of a mistyped URL, we chose not to link directly to the Tor project on the Strongbox page in order to make it less likely that a source's access to Tor could be traced back to *The New Yorker*, which could potentially compromise his or her anonymity. Similarly, mirroring a copy of the Tor browser bundle or hosting a D.V.D. image of the Tails anonymity VM software, while potentially offering a marginal degree of additional security to the source at one juncture, engenders security implications for newyorker.com at another juncture. Other issues involve compromises that, for practical reasons,

we are unable to make at the current time.

A final concern noted in the report is that messages sent by your team as tests did not receive requested responses with a code. The messages had in fact been received, but the team checking Strongbox believed they were part of a separate test – one of many conducted internally – and did not realize that they required additional action. They have now responded, and we look forward to hearing the results of the test and seeing them reflected in your audit – and, of course, we are ready for you to test the service again, at any time.

As you know, building any system requires making choices. In ours, we have attempted to devise the most secure system practicable while keeping it usable for sources as well as journalists. In the documentation, we have been as transparent as possible about the specific kind of security Strongbox offers for anonymously transmitting documents. We cannot lock down a source's computer to create an absolutely secure system nor can we mitigate or take responsibility for his or her actions. But we have worked to provide a system that offers a better way to anonymously submit materials.

We will continue to work toward making Strongbox even more secure and easier to use. Your comments and suggestions are a valuable part of helping us move toward that goal.

Sincerely yours,

Nicholas Thompson
Editor, newyorker.com