Hello, I am a professional security consultant for a company with public clients including Mozilla, Microsoft, and Apple along with many Fortune 500 companies. We work hard to protect the best companies out there which face serious threats.

I believe the settlement the FTC has made overall has great intentions. I disagree with some of the terminology and the recommendations that were made to twitter. And I will explain why.

First, the statement says that twitter `deceived consumers and put their privacy at risk by failing to safeguard their personal information`.

What was the deception exactly? Twitter made no claims to be perfectly secure. They had a security policy in place with passwords for administrative access. Furthermore, twitter was perfectly honest about both compromises and very clearly and very publicly announced what happened within an extremely short timeframe. They went above and beyond in terms of honesty and transparency. Something they should have been commended for instead of ridiculed.

Next I would like to discuss the recommendations. As twitter was a quickly fluctuating and experimental technology, they had a wide attack surface. There were 2 public compromises that likely brought the attention of the FTC. The first attack resulted from a guessed password a user who was unknown to have administrative privileges until they were compromised. Admittedly, a better password policy would have had some chance of preventing this. But the second attack was not possible to defend against.

One of the administrator's email account was compromised. The majority of the recommendations made by the FTC center around this attack especially.

* require employees to use hard-to-guess administrative passwords that they did not use for other programs, websites, or networks;
* prohibit employees from storing administrative passwords in plain text within their personal e-mail accounts;
* suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts;
* provide an administrative login webpage that is made known only to authorized persons and is separate from the login page for users;
* enforce periodic changes of administrative passwords, for example, by setting them to expire every 90 days;
* restrict access to administrative controls to employees whose jobs required it; and
* impose other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses.

If the email account of an administrative user is compromised, why would any of the recommendations above work? The truth is that once an email account is compromised everything else falls through. Plain text passwords being stored are a minor detail at that point. From there an attacker can reset passwords or other credentials trivially, but they could do something more subtle. They could pivot their privileges to gain full control over that administrative user's machine where he or she is checking their email from. From there, all of your security recommendations fall a bit short.

As a consumer, I would like to see the FTC protecting user privacy on a much more important domain. I think you know what I am talking about when I mention Facebook. Their business practices can easily be construed as deceptive. Pictures that users upload and delete...do not get deleted. They store user information indefinitely. It becomes their property. The information facebook collects loses all guaranees of privacy as it is sold to marketing agencies to companies probably similar to axciom. In addition, they practice predatory user interfaces that make deleting your account difficult. They do (or did) deceptive things such as placing images of people from your social

network with dialogues saying that "Kate will miss you" or "Roger will miss you" or your brother "John will miss you".

I think if the FTC were to do something really great for social networking, they wouldn't attack companies like Twitter. Twitter essentially has little PRIVATE personal information besides an email address and most people use twitter with this in mind. Instead, the FTC should focus on the more critical business practices which collect social networking information about us and are unwilling to discourse how it is being stored managed and sold.

Thank you. I would greatly appreciate a well formed response.