Social Media in Business: A Double-Edged Sword Too Deep

Kristof Marsolais

San Jose State University

Author Note

Include any grant/funding information and a complete correspondence address.

Abstract

This is the analysis of a repeated cycle of inattention to security prevention methods. The first incident occurred through email and was followed by the popular trend of social media. While the former was not as severe due to the technology and accessibility of the given data, the latter's tempting offer of social connection and communication with the world amplified the inevitable danger of exposing our identities to the world that compromised the livelihoods of individuals everywhere. One has to wonder what factors played into the hands of hackers who now have our information on top of the corporations who took ours. Because of what the founder of Facebook has done, we now have a bigger mess to clean up. We have to implement security and privacy policies that are not so easily accessed. Our job is only beginning.

Social media is a booming technology which has billions of users using it every day. I was one of them and had multiple Facebook accounts over the years. I would go through a cycle of deleting my Facebook profiles every 5 years or so. The reason I did this was because I changed with each cycle and had a very different perspective on each profile, so I constantly changed it. I deleted my Facebook for the last time in April 2019 after reading about the Facebook breaches of September 2018. A significant amount of personal information became accessible and many individuals had their livelihoods at stake. I will discuss in detail both the pros and cons of datamining, one of social media's most common marketing tactics. I will then follow with an explanation of what happens when you try to leave Facebook and what actually results from experience. After explaining the results of deleting my Facebook account, I will talk about the history of Email, the predecessor of social media and how it impacted both my life and the individuals who participated in it. I will finalize my report by explaining the severity of data breaches and how they can spoil the reputation of a social media company and the varying consequences it can have on its users. Social media has become a liability rather than a luxury due to the lack of prevention measurements, information security and privacy protection.

The data breach of 2018 was not the only instance where Facebook has had a breach of information or has failed to consider the privacy of its individuals. It has even gone as far as scanning the information of your specific device as Facebook states in their terms of usage: "As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or

features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device" (Facebook, 2019). Basically, my entire device is scanned and anything on the device is accessible to their database. Your device gives you a notification saying, "Allow Facebook to access Photos" and "Allow Facebook to know your location" and you can decide whether you want them to have that access or not. Facebook's functionality however expects you to say yes to both and not enabling those permissions makes navigating and using Facebook incredibly difficult. Now one device being accessed by a social media chain like Facebook may not necessarily be harmful to businesses that are smaller and do not have databases that would compromise their products, but it can have ramifications for much bigger companies that are trying to hide information about their product until a specific release date. I'll give a hypothetical scenario to further explain the severity of how social media can sabotage the secrecy of a given product and can jeopardize and possibly alter the final product. Imagine that you are a video game tech company and you have plans to release a new video game that is anticipated to be one of the top-selling games of the year. You have developers in your team who have signed a non-disclosure agreement not to reveal the material of the given game until its initial release. The issue is that some of the employees decide to tell their loved ones or friends about what they are working on using the Facebook application known as Messenger. The information that is stated in that conversation can be sold to datamining groups that love to reveal content of video games before the expected date release.

In some cases, this is perfectly okay and companies like Blizzard Entertainment have followed this practice on purpose to develop hype for their future games. It's because of datamining that Blizzard has often made certain changes in their video game of World of

Warcraft in response. They published an article on their sit, Blizzard Watch, that mentions how datamining, while interesting, doesn't make guarantees to their final product. In an article by Matthew Rossi, he stated: "This is one of the dangers of taking datamining too seriously — while we can discover all sorts of cool and interesting things looking through those files, it doesn't mean that Blizzard will implement them, and even if they do, they can make changes right up to the day those files go live and become part of the live game" (Rossi, 2019). With a company as big as Blizzard this is more than possible. Anybody analyzing the early released content may think that the game is going one way, but instead the video game can alter that idea at the last second because Blizzard has the staff and the resources to make it so. While this is possible for Blizzard, other game developers do not have the luxury or the resources to recover or handle datamining information on this scale. This was the case with the creators of The Binding of Isaac: Rebirth when their game was datamined. An interview took place on a stream on Vinesauce where the creators of the game were angry with the fact that the months of development it took for them to place secrets into their game were revealed within a week (Valentaten, 2014). It was disheartening to them that they could not place secrets or make the game challenging because datamining groups would have early access to the information and spoil it. The developer Edmund McMillen said: "I think I've learned that there's no point in really doing that stuff, and the best way to hide a secret is to lock it in a very challenging area. I think if we end up doing anything like that in Rebirth, it'll just be behind a barrier of entry; having a certain amount of skill" (Valentaten, 2014). He was forced to make changes in his product because individuals were able to reveal secrets that he wanted to be kept private until release, and he found it challenging to make the changes because of curious fanboys.

What is true in the scenario related to Messenger is the fact that the messages and conversation can be accessed and viewed by the executives of Facebook. Your conversations in Messenger are scanned and your personal life is completely accessible to the administration of Facebook (Frier, 2018). The reasoning for this is to prevent individuals from sending malicious software, links or hate links to people on the application. That is stated in their data policy as: "We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products" (Facebook). It sounds like an honorable sentiment because Facebook users want their client base to have a secure and social environment for business purposes. Unfortunately, that also means significant monitoring as they stated in their terms. You are probably thinking that maybe if you leave Facebook like I did, they will stop monitoring your information. This is not necessarily so, because in another section of the terms of use policy, they stated: "We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted - whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months" (Facebook, 2018). Why would they need to maintain your information for 6 months unless they were planning on using that information for something before you left for good? When I deleted my account, they stated that my account will be deleted within thirty days. If my math is correct that is approximately one month, a sixth of the time that Facebook holds on to your data. If your ex held your personal information and record of everything you said, posted, and shared media with, you would feel

uncomfortable if she sold that sensitive information to companies that may try to sell you products that you thought of, but really did not want. I have deleted my Facebook at least three different times and created new Facebooks within the years of 2009 through 2019. Through each of these cycles I would have different friend suggestions based on the people that I knew at the current time. What I did not expect was the group of friends that I was trying to avoid kept showing up in my recommended "add friends" groups and I was wondering why that was the case. It turns out, that Facebook never actually deletes the information from previous files just in case you want to return. Even if Facebook did go through the effort of deleting your profile within a reasonable time, that information would not be erased from the entirety of the Internet. Someone like me, Reg Harnish, also deleted his Facebook account and shares the same skepticism that it really will not do too much to prevent the damage that Facebook has already done. He said: "Deleting my Facebook account will not remove the "shadow profile" that exists about me. Thousands of pages of data will remain in Facebook's archives for the foreseeable future. Not to mention, my family and friends will continue to provide Facebook with pictures and other updates about me that will build upon my online profile. In some cases, Facebook will continue to collect information about me through ads all over the internet. It's nearly inescapable" (Harnish, 2018). He is correct about this. We are in a world where our personal and private livelihoods are no longer private or personal, due to developments in this technological era. Our connections require our personal information on a massive scale. As we proceed to obtain any services in future enterprises, any mistakes that we made in the past, present or even future are made public. We cannot keep things private. Facebook and other social media platforms are becoming essential in business connections because they offer services that make connections easier and more convenient for consumers and businessmen alike. The primary issue

with the rise of social media is the same issue that E-Mail had during its developmental period: security measurements.

I remember having an email account in Yahoo.com as early as 2004. That was my freshman year in high school and I used that email to send information and also linked a significant amount of services to the specific email. I had an unprofessional name attached to it because it was my first email and I did not know any better. I remember deleting that email in 2008 and replacing that email with an email that had my first and last name attached to it. Applications like Facebook, Myspace, World of Warcraft and your academic registration into community college required having an email. I learned that I needed more than one email, because reading all of the emails was incredibly overwhelming and looking for essential information was difficult when trying to figure out a deadline for an assignment or final exam. David Crocker, a member of the ARPANET research community, agrees. He stated in an article: "In the 1970s, it was extraordinary for a person to receive as many as 50 messages a day. Today, it's not unheard of for an individual to receive 1,000 messages a day. Although basic e-mail requires only simple technology, it is challenging to scale e-mail and make it an essential service for a large pool of users. Doing this requires adding functionality, designing a good user interface (usability), and providing non-stop reliability while delivering messages quickly" (Crocker, 2012). We get a significant amount of advertisements and spam email as well which is also dampened when you split your email into two accounts. Spam filters are now available on your email accounts and reading through your email is easier than it was before. There were two providers for email that I used during my academic years at Mesa college. I made my primary email on Yahoo and my gaming one on Google. I would have never speculated that the former would be the email that I would dispose of. It was a generally new technology, a way of sending

significant amount of information to individuals instead of meeting them in person. Crocker explained in a “Today, the e-mail equivalent of the USA Postal Service is provided by independent, interconnected private providers, such as your Internet access service and your employer. The typical machines that are used often process many millions of messages per day, delivering these messages within minutes or seconds and suffering only a tiny fraction of failed deliveries (Crocker, 2012). Just think about how useful that is; you can send a significant amount of information that a regular memo delivered to an individual would take much longer to do. With the technology being invented in 1975 and its significant evolution, there were bound to be barriers and roadblocks that would impact its development.

Email was invented during a time period where internet security was not the highest priority. The world wide web was not fully accessible to the public until some time during the 1980s and the email system was a little more refined at that period. Despite the advancement made to the system, it was still not enough to compensate for the vulnerabilities, and it would not be long until someone decided that they could exploit those vulnerabilities in the network. That network was Yahoo’ system and it began in 2014 and supposedly ended in 2016. While Yahoo has not given an official statement of how the email breach had occurred, Randy Battat, an Email security provider, hypothesizes that the breach may have occurred “likely through spear-phishing attacks in at least some instances. In such an attack, a user with access to Yahoo’s internal network receives what appears to be a legitimate message that invites them to click on a link, which then secretly installs malware on their computer. Presumably, the compromised computers ultimately provided the attackers with access to the Yahoo network” (Battat, 2017). Learning about the attack this semester made me delete my yahoo email account because the likelihood that my account was compromised. In the same way that deleting my Facebook does not mean

that I will be erased from the web, my Yahoo email details continue to be available. What this also means is that the information that any hackers potentially gathered from my Yahoo account is now in their database and it could be used against me in the future. Something to note in Randy's analysis of the breach is that the hackers could have easily targeted individuals and gained access to their accounts and begun farming the information from the victims themselves, however there was a much bigger opportunity to be had by targeting the administration's systems because doing so would make the harvesting of accounts much easier (Battat, 2017). He gave a list of vulnerabilities that made breaching Yahoo relatively easy for the hackers to gain access to their servers. The most important one was vulnerability of the User database (UBD). This contained all of the personal information that was connected to each of the email accounts. While the passwords on the given accounts were not revealed on these databases, they could be accessed because the hacker could look up information retaining to their account and used that information attached their emails and bypassed security protocols because that information was available. If that was not scary enough, they also revealed your alternate email in case your email was compromised. While this did not affect me on a personal level, it damaged a significant amount of people on a business level. Battat stated: "As these were often company email addresses, once the attackers had a copy of the UDB, they could search for the domain names of the companies where their targets worked. Sometimes the alternate email addresses included family members, who could also connect the attackers to their targets by association. Password challenge and response questions provided helpful hints in penetrating not only Yahoo, but other systems as well" (Battat, 2017). If a hacker has access to your personal information and knows the answers to your security questions, what is to stop them from resetting your password then using the password to access your account, then use that account to see all the information within

the account and continue to exploit it further? That's exactly what happened, according to Battat: "Armed with this information, the attackers then penetrated certain Gmail accounts by logging in, answering the challenge questions, and responding to a confirmation email sent to the now-compromised Yahoo recovery account. Even though the Google and Yahoo passwords themselves were never revealed, the operations around them were compromised, and so the accounts were breached" (Battat, 2017). Yahoo never told me if my account was compromised or if it was breached, and my associated Gmail account, which is my gaming account ,may have been compromised because of it. Fortunately, because it is my game account they did not find any information in it that had anything to do with my Social Security number or identification that would compromise anything but my debit card. I looked at my emails during that period and did not find any information that revealed my debit card information, only confirmations of games that I bought that year. Yahoo was not the only email provider who suffered a significant breach. In the year 2018, Google had announced that there was a vulnerability in its application known as Google+, an app meant to compete with Facebook. Then I remembered how Google+ really wanted me to sign up for it in 2016 and I was relatively annoyed by the fact that it was unrelenting in its need to be acknowledged. It suffered a breach in March of 2018 very similar to Facebook's data breach years earlier. Although the damage was not as severe as Facebook's breaches were, there is something still troubling about the way the breach was handled. An article from the New York Times stated: "Steven Andrés, a professor who lectures about management information systems at San Diego State University, said there was no obvious legal requirement for Google to disclose the vulnerability. But he added that it was troubling — though unsurprising — to see that the company was discussing how reporting the vulnerability might look to regulators. There is no federal law requiring companies to disclose a security

vulnerability. Companies must wade through a patchwork of state laws with different standards" (Wakabayashi, 2018). It's not uncommon for a company to want to hide embarrassing information about one of its possibly flawed projects. Every company has a project that they are embarrassed about, and they do not want to talk about it to the public. It's like me when addressing my mother about the cleanliness of my room. I will fix the issue eventually, but I should do try to take care of it before my mother sees how dirty it has become since the last check. The actual damage done during this mishap may not have been significant, as this passage from the article stated: "Introduced in 2011, Google Plus was meant to be a Facebook competitor that linked users to various Google products, including its search engine and YouTube. But other than a few loyal users, it did not catch on. By 2018, it was an afterthought. Google would not say how many people now frequent Google Plus, but it said in the blog post that the service had low usage — 90 percent of users' sessions are less than five seconds long. When Google's engineers discovered the vulnerability, they concluded that the work required to maintain Google Plus was not worth the effort, considering the meager use of the product, the company said. Google said it planned to turn off the consumer version of Google Plus in August 2019, though a version built for corporate customers will still exist. The failure of Google Plus has relieved Google of some pressure on issues faced by Facebook and Twitter, particularly Russian disinformation efforts" (Wakabayashi, 2018). It was users' general disinterest in the service itself that saved the compromised accounts from being too damaging. It's hard to determine if Google would have continued using Google Plus if the platform was popular. Google is making a financial decision to shut down the program and does not seem to be shying away in the press from saying it is also for moral reasons.

While an unpopular social network platform breach like Google Plus did not make a huge splash, Facebook's data breach has an alarming ramification for many users because of its popularity and the personal information that has been revealed. I mentioned earlier how Facebook can scan your devices and listen in on your conversations. I also mentioned that Facebook, much like e-mail, acts as a core necessity to certain applications such as Pokemon Go, Instagram, and various dating apps like OKCupid. Some of these applications have micro transactions that often store your payment history and if you purchased anything on those apps Facebook will record it. Like Yahoo, Facebook did not make an announcement as what you should do with your Facebook account in response to what happened in this initial security breach. I thought my compromised account was bad enough, but it turns out my account's breach was lackluster and minimal compared to the significant damage it had for Facebook reliant users as the New York Times explained. "Three software flaws in Facebook's systems allowed hackers to break into user accounts, including those of the top executives Mark Zuckerberg and Sheryl Sandberg, according to two people familiar with the investigation but not allowed to discuss it publicly. Once in, the attackers could have gained access to apps like Spotify, Instagram and hundreds of others that give users a way to log into their systems through Facebook. The software bugs were particularly awkward for a company that takes pride in its engineering: The first two were introduced by an online tool meant to improve the privacy of users. The third was introduced in July 2017 by a tool meant to easily upload birthday videos" (Isaac & Frenkel, 2019). Regardless of how severe you may think the bugs to the system were, any bug that makes the top individuals of the platform vulnerable should have been considered before implementing it into the public. This breach has harmed the safety and trust of over 50 million users and has generated a significant amount of concern over the future of its integrity.

To add insult to injury, this is not the first time that Facebook has encountered a data breach scandal that would question the safety and protection of its users. “In April, Mr. Zuckerberg testified about revelations that Cambridge Analytica, the British analytics firm that worked with the Trump presidential campaign, siphoned personal information of millions of Facebook users. Outside the United States, the impact of disinformation appearing on Facebook and the popular messaging service it owns, WhatsApp, has been severe. In countries such as Myanmar and India, false rumors spread on social media are believed to have led to widespread killing” (Isaac & Frenkel, 2019). I remember growing up and in 1999 there was the Columbine High School shooting on April 20, 1990 and I remembered the media going berserk about what the rationality was. One of my teachers in class blamed a game called Doom which a is first-person shooting video game. This article from the New York Times has speculated that false propaganda and cyberbullying through their applications may have harmed or killed people in the real world because of attempts to shut down. It is significantly plausible that it may have been responsible for deaths in the United States. With cyberbullying on the rise due to the increased confidence of hiding behind a screen, it is highly plausible. Facebook does have a zero-tolerance policy to hate speech and will censor it if it violates their terms. “When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm” (Facebook 2019). The breach situation had proliferated to such an extent that even Facebook users who tried to notify their friends could not even get the word out. The conclusion of the article stated: “Users who posted breaking stories about the breach from The Guardian, The Associated Press and other outlets were

prompted with a notice that their posts had been taken down. So many people were posting the stories, they looked like suspicious activity to the systems that Facebook uses to block abuse of its network. “We removed this post because it looked like spam to us,” the notice said” (Isaac & Frenkel, 2019). Facebook had blocked all posts of the breach on their network because they claim that it was spam. It does not bode well for a company that offers an effective way to communicate with friends and keep in touch with people that it blocks posts about a pending disaster. I understand the reasoning for blocking those posts for legal reasons, but it would have been more useful to give the users information on how to secure their profile. Or, they could have explained why they were taking down posts or not communicating with users just then. A lack of communication with clientele on a system that is specifically designed to make communication and meeting much easier negates the entire purpose of the given product. Mark Zuckerberg stated that this program was meant as a way for people to communicate, a way for people to learn more about each other and understand each other like never before. What he failed to take in account was that overflow of metadata that was posted on his website would generate value for hackers to infiltrate. When you boast a database of a significant number of individuals, including those who have business ties with larger corporations, an attack is inevitable and security measures need to be considered.

Facebook’s development accelerated a significant liability in the data management business. They focused on generating a significant amount of information for a low cost. It’s rather ironic because this was a concern in the profession of record keepers. “Just when compliance and records managers thought they had nailed down information governance for e-mail, IM, and electronic records—social media came on the scene creating new, dynamic challenges. “Tweets are no different from letters, e-mail, or text messages—they can be

damaging and discoverable, which is especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors. Yet another compliance headache is born" (Smallwood, 2014). All the fears and concerns that society had about in the development of e-mail – the lack of security protocol, the lack of damage control, risk auditing, and crisis management, were all things that Facebook turned out to inherit as well.

It does seem rather awkward that employees in corporations are being told to follow guidelines for a social media platform that is currently falling apart. Some of the guidelines stated in the Smallwood text have incredible merit. One of the guidelines stands outs specifically and for a very compelling reason. "Train, train, train. Social media is a new and immature technology that changes rapidly. Users must be trained and that training must be updated and reinforced on a regular basis so that employees are clear on guidelines, understand the technology, and understand the business objectives for its use" (Smallwood, 2014). Try to imagine this scenario. We are telling our employees to train for an unpredictable social media technology that even the founders of that given technology cannot understand, let alone contain. The same employees that are being told to understand the technology are also expected to react and prepare for the events of a data breach that hits the social media technology that is not under their control. Even if the employees mastered the guidelines that made them absolved of any controversy in their company, you still expect those employees who had suffered the current data breach to keep their cool? That's an insane expectation for a technology that is as volatile as Facebook. Nobody ever posts a perfect post and every individual has a moment of error or irrationality and often posts something they regret.

The problem is that Facebook does not let you forget. Any mistake you make on their platform they remind you of constantly. For example, if a woman suffered a miscarriage, she

would still suffer the pain of seeing ads for baby products because of her search history on her mobile device. I mentioned earlier that Facebook scans all your devices and the history connected to it and this is the real issue with that technology. Datamining ruined the potential of a video game by spoiling the secrets of the game. Although Blizzard Entertainment's content was revealed, they had a damage control method that would prevent their game from being completely spoiled or at least ensuring that their content never left the building. We were promised a technology that would give us connection to the communities of our choice, and we paid a significant price for it: our privacy. Mark Zuckerberg has announced that he wants to make the future of his platform private and that users will be able to have that privilege. That would have been great ten years ago or even as late as 2016. If Facebook wants me to sign up again, it's going to take a significant amount of time for them to gain my trust back. I didn't expect my personal information to be a commodity that they would share with corporations waiting to sell me something. The way Facebook managed it is not professional and not worthy of a basic information standard. Not deleting the information immediately after 30 days is a violation of trust and does not make sense in a retention-based system. If a file becomes obsolete, you do not keep that file unless you want to make it historical and hope to profit from the use of that record. Since the company has not completely deleted my information and kept it for so long, I can only assume it is going to continue selling my inactive information because it needs that profit margin. By keeping this record, they continue to endanger consumers' livelihoods, proving that outdated content is more important than my safety, and creating a liability across any of my future endeavors with these apps.

References

Battat, R. (2017, October 2). Risk management – lessons from the yahoo hack. Retrieved from http://www.rmmagazine.com/2017/10/02/lessons-from-the-yahoo-hack/

Brenneman, K. (2017). Preserving e-mails with historical value. Information Management Journal, 51(2), 36-39. Brenneman 2017.pdf

Crocker, D. (2012), "A history of e-mail: collaboration, innovation and the birth of a system", The Washington Post, 20 March, available at: www.washingtonpost.com/national/on93 Correspondence as a documentary form Downloaded by San Jose State University At 08:16 29 August 2015 (PT) innovations/a-history-of-e-mail-collaboration-innovation-and-the-birth-of-a-system/2012/ 03/19/gIQAOeFEPS_story.html (accessed 10 October 2014).

Frier, S. (2018, April 4). Facebook Just Confirmed That It Reviews Your Private Messages. Retrieved from http://money.com/money/5227844/facebook-reviews-private-messages/

Facebook. (2019, April 19). Facebook Data Policy. Retrieved from https://www.facebook.com/policy.php

Harnish, R. (2018, June 18). I Deleted My Facebook Account And It Doesn't Mean A Thing. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/06/18/i-deleted-my-facebook-account-and-it-doesnt-mean-a-thing/#5d86c9948e8f

Heil, J., & Jin., S. (2017). Preserving seeds of knowledge: A web archiving case study. Information Management, 51(3), 21-24.Heil 2017.pdf

Isaac, M., & Frenkel, S. (2019, March 19). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. IT Professional, 14(5), 53-55.pdf

Rossi, M. (2019, April 18). Why datamining is fun, exciting, and not to be trusted. Retrieved from https://blizzardwatch.com/2019/04/18/datamining-fun-exciting-not-trusted/

Smallwood, R. (2014). Information governance: Concepts, strategies, and best practices. CHAPTER 13 Information Governance for Social Media

Valentaten, D. (2014, November 13). Datamining Ruined The Binding of Isaac: Rebirth Secrets. Retrieved from https://segmentnext.com/2014/11/13/datamining-the-binding-of-isaac-rebirth-secrets/

Wakabayashi, D. (2018, October 11). Google Plus Will Be Shut Down After User Information Was Exposed. Retrieved from https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html

Zhang, J. (2015). Correspondence as a documentary form, its persistent representation, and email management, preservation, and access. Records Management Journal, 25(1), 78-95.RMJ 2015 Zhang Email.pdf