Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 3 (2015) 1101 – 1108

Procedia MANUFACTURING

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

Cyber security and user responsibility: surprising normative differences

Bradley J. Strawser[a,]*, Donald J. Joy, Jr.[b]

[a]*Naval Postgraduate School, PO Box 7155, Carmel by the Sea, CA, 93921, USA*
[b]*University of Alaska, 9122 Eagle River Lane, Eagle River, AK 99577, USA*

Abstract

High-profile hacking incidents caused critics on social media to blame the celebrities who were hacked rather than the hackers. They claimed that those whose risqué photos were stolen were to blame for failing to secure them. While such attempts to blame-shift can be dismissed as victim-blaming, they elucidate a set of questions about the ethics of personal responsibility as it relates to computer security. Is the normative standard for security in the cyber realm in any way significantly different than the moral norms governing all other aspects of life with respect to questions of individual responsibility, blame, and negligence?For example, if I lock my possessions in my home, I have a reasonable expectation that they are safe from theft. But even if my house isunlocked with my possessions visible, few would argue that I deserve to be robbed due to my failure to secure my valuables. It would be an implausible stretch to assert that my negligence constituted a lack of blameworthiness on behalf of the thieves, or provided any mitigation to the moral wrongness of the act of robbery. Consider another more poignant example for the cyber world. Imagine a man walking through a neighborhood checking doors to see if they are unlocked,but not stealing anything. Few would consider such behavior acceptable within present societal norms. Yet, in the cyber world, such norms have significantly less traction.Such thinking raises two important questions. First, does the average person have the wherewithal to implement adequate or effective computer security? Second, whatever the cyber-equivalent to the norm of traditional security is, is there a prevailing belief that failing to meet it is a matter of negligence in the cyber case where the equivalent failing would not be considered negligent in the non-cyber case? Or, in other words, if a computer user's data is compromised did she, in some sense, "get what she deserved"?These questions have significant ethical and practical implications for cybersecurity and human factors.

Peer-review under responsibility of AHFE Conference

*Keywords:*Cyber security; Individual responsibility; Normative standards; Hacking; Data theft; Human factors in security

* Corresponding author. Tel.: +1-831-656-2440.
E-mail address: bjstrawser@gmail.com

Peer-review under responsibility of AHFE Conference
doi:10.1016/j.promfg.2015.07.183

1. Cyber security and user responsibility: surprising normative differences

As 2014 drew to a close, two high-profile cyber hacking[1]incidents dominated news headlines. The first one, dubbed "the Fappening," took place in September and involved the theft and publication of dozens of digital photographs and videos depicting Hollywood celebrities nude or engaging in sexual activity [1]. Then, in December, the news broke that Sony Pictures Entertainment was hacked just prior to the release of the motion picture *The Interview* [2]. Both incidents involved the wide dissemination of personal, private, and sensitive information via the internet. Another similarity that these cases shared was the apparent lack of public sympathy for the victims.

In the wake of these high-profile hacks, a large number of people took to social media to lay blame on the victims rather than the hackers who stole and released the data. The common sentiment these critics advanced was twofold: 1) The nature of the compromised data was such that the victims should have known that they would be targeted for theft; and 2) Because they should have known that they would be targets of hackers, the owners of the data ought to have done a better job of protecting it. Hence, Sony Pictures and the exposed celebrities were – at least in part – blameworthy for the events due to the very nature of the digital property that was stolen. In other words, these critics claimed, things such as sensitive emails, executive correspondence, and especially risqué photographs are such desirable targets, that the mere *possession* of such data could implicate some level of culpability if their security is compromised. When coupled with the victims' inability to secure their data (as evidenced by the fact that the data was able to be stolen), the fallacious conclusion broadcast in the court of public opinion was that the victims had at least a share in the blame for what had happened, perhaps through negligence. Moreover, this assigned blame on the victim is taken (by some) to partially mitigate the blameworthiness of the cyber-criminals themselves.

There are myriad problems with this sort of blame-shifting and victim-blaming, some of which we will address in this paper. But, as mean-spirited as the attacks may be, they elucidate a compelling and important set of questions about the norms of personal responsibility as they relate to computer security. To see this, let us first assume that there is some normative expectation for individuals to take reasonable efforts to secure their possessions, such that failing to do so can constitute proper conditions for negligent blameworthiness if that security is compromised. Call this the "norm for individual security of property," or NISP, for short. Here then is the question these cases press: is the NISP in the cyber realm in any way significantly different than the NISP which governs all other aspects of life? These recent cases of cyber hacking, and the public response to them, suggest that the answer is unclear, at best. In this paper we will explore this surprising possibility and some of the important moral implications it raises for cyber security.

2. Whythe type of data one possesses should not contribute to one's blameworthiness

Before we delve into questions about security related normative standards, it's important to first dismiss the assertion that data-theft victims may be culpable merely because of the type of data that is stolen from them. Victim-blaming is not a new phenomenon and it's difficult to know precisely why certain crimes tempt people to look toward the behaviors of the victim when in search of moral explanation. This tendency seems especially pernicious in cases where we do not know all the facts. Something motivates us, perhaps, to want to fill in the epistemic gaps and place things into categories like victims, culprits, motives, alibis, and the like.

In the case of the nude celebrity photos, it was easy for some to immediately assign blame on the women for having nude and explicit pictures and videos to begin with for "making themselves targets." After all, no hacker has ever infiltrated our cloud storage and 'leaked' one of our Logic PowerPoint lectures. The common refrain across social media was, "if you don't want your nude pictures stolen and made public, then don't have nude pictures!" While we admit there is a prima facie case to be made for the idea that possessing X is a necessary condition for having X stolen from you, that's about as far as one can logically take the line of reasoning before encountering some serious problems of consistency.

---

[1] Although it is debatable how many of these breaches of data qualify as bona fide instances of hacking, we will use the term "hack" throughout this paper to describe any unauthorized access to personal data without the explicit consent of the data owner.

In our present cyber age, nearly every adult has some form of sensitive electronic data stored somewhere. Whether it's personnel records at their jobs, financial credit data at their banks, or even simply the mundane personal information that is unique to each of us (address, telephone number, Social Security number, information about one's families, etc.) nearly all have data about ourselves that we would probably rather not be made public. Yet, of course, if one's bank account were compromised by a hacker, it would be ridiculous to assert that "if you don't want your money stolen, then don't put your money in the bank."

It is clear that certain types of digital data are more attractive to thieves and hackers than other types. The desirability of the data may be based on what the data itself contains or, in some cases, who owns the data. For example, financial data, trade secrets, and internal emails from a large company like Sony Pictures are likely a bigger target than our Logic PowerPoints or videos of one of our cat's chasing a laser pointer. Likewise, a thief would be wiser to target the bank account of our 40-year-old selves rather than our 20-year-old selves (assuming the thief is looking for money).

Furthermore – as anyone who has ever glanced at the 'literature' at the grocery checkout line can attest – our celebrity-obsessed culture has created an industry out of the 'voyeurization' of celebrities. Seeing photographs of movie stars buying lattes without makeup or walking their dogs has become a 'legitimate' form of entertainment for some. The demand for candid celebrity photographs fuels the multi-million dollar paparazzi industry.2 In a world where this behavior is viewed as business as usual, it is hard to imagine what kind of photos or videos a celebrity could reasonably possess that would not make them targets for data theft.

In short, it doesn't follow from the fact that some data is more desirable, that one is blameworthy merely for possessing it. If that were the case most of us (especially anyone with even a modest level of celebrity) would be 'guilty' of possessing tantalizingly hack-worthy data. Further, there is no other circumstance where the mere possession of something that is desirable to others is tantamount to shared culpability for its theft. Nobody blames the burglary victim because her television was 'too nice.' Likewise, similar blameworthiness claims about the victims of cyber data theft are equally erroneous – regardless of who they are or the nature of the data that is stolen.

3. A proper standard for 'traditional' security

The second major criticism waged against the victims of these hacks was that they were culpably negligent for failing to do a better job of securing their data. In other words, if you know that you have sensitive digital information that you don't want stolen, then it is your responsibility to properly secure it. Failure to exercise a reasonable level of due diligence, constitutes a failure on the part of the data-owner.

Such thinking raises two interesting questions for cyber security and the NISP. First, does the average person have the wherewithal to actually implement adequate or effective computer security – whatever the proper NISP for the cyber realm should be? Second, whatever the cyber-equivalent to the traditional NISP is, is there a prevailing belief that failing to meet that norm is a matter of negligence in the cyber case where the equivalent would not be considered negligent in the non-cyber case? Or, in other words, is there a consensus forming that if a computer user's data is compromised that in some sense she "got what she deserved," that would not prevail in our non-cyber norms? Is the cyber-NISP more demanding than the traditional NISP?

When it comes to matters of 'traditional' (non-cyber) security, the standards of due diligence *seem* clear and fairly straightforward. For example, if I secure my possessions in my locked home (or even better, a locked safe within my home), I have a reasonable expectation that they should be considered outside the reach of my fellow citizens.But even if I take none of those precautions and instead leave my front door unlocked with my flat screen television clearly visible from my front window, few would argue that I *deserve* to have my house robbed and my TV stolen due to my failure to secure my valuables. If my television were stolen under such conditions, it is true that many might contend that I was negligent in my home security. But it would be an implausible stretch to assert that my negligence (if, indeed, it was negligent) somehow constituted a lack of blameworthiness on behalf of the thieves, or any kind of mitigation as to the moral wrongness of the act of robbery itself.

---

[2]For example, in 2012, Angelina Jolie and Brad Pitt sold several tabloids photos of their newborn twins for $14 million (which they donated to charity) [3].

However, it is true that after a burglary occurs, as part of the normal crime investigation, it is reasonable to ask whether the doors and windows were locked. If the answer is yes, then we view the robbery as an unfortunate incident and the person who was robbed as a 'real' victim. If the house were left unlocked, we may still be sympathetic, but simultaneously think that by not taking the steps to lock doors and windows that the victim didn't do enough to deter a would-be-thief. Call this later case the 'negligent' victim. But this conclusion is perplexing because it seems that a 'real' robbery victim who locked her doors also did not do enough to sufficiently deter thieves either, as evidenced by the fact that she was still robbed. Moreover, even if both the 'real' and the 'negligent' victims failed to deter thieves, that is still a far cry from actually contributing to or being culpable in some way for the robbery. We view the two situations differently, but what is the relevant distinction if it is not effective theft prevention?

In both cases the victims suffered an injustice and an invasion of privacy at the hands of a burglar. In neither case is the moral impermissibility of the burglar's actions in doubt. Yet, in the former case, our intuitions lead us to be (at least marginally) more sympathetic to the victim than in the latter. Perhaps this hinges on a belief that the victim's own actions *could* have played a role in preventing the injustice (even though they didn't in either case). The irony in this example of traditional security is that locking one's doors is generally accepted as a reasonable attempt at security even if it actually does little to stop a determined burglar. Note well:here the belief that a person has done enough and met the NISP seems linked to the token effort of using the security measures at their disposal *rather* than on the actual efficacy of those security measures. Importantly, regardless of whether the homeowner meticulously locked the house or inadvertently left the front door ajar as she rushed out, in neither case, of course, is it reasonable to conclude that she deserved to be robbed.

So the question remains, if the adequacy of traditional security to meet the NISP is not tied solely to its effectiveness, then what does it depend on? Does it really come down to simply 'making an effort' as the foregoing example suggests? To further examine this question, let's imagine two rather extreme examples. Mr. Stronglocke is a traditional security aficionado. All of his doors have multiple locks, deadbolts, and chains. Both his doors and windows are hooked up to state of the art alarm systems and the signage advertising those security systems is prominently displayed in an effort to dissuade any potential burglars. Mr. Carefree prefers the honor system. Mr. Carefree does not have any locks on his doors or windows, and the only sign that he displays reads, "My home is unlocked and I have some nice stuff inside, but I would prefer that you not enter and steal any of it (especially, the new XBox in the den). Thank you."

If we were told that one of these houses was burglarized, it would not be surprising to learn that it was Carefree's house instead of Stronglocke's. Stronglocke clearly exhibited a level of vigilance that Carefree did not and in this case it seems to have paid off. But does this thought experiment tell us anything about what the 'appropriate' level of due diligence ought to be? If the efficacy of the locks was not an appropriate measure in the first example with the 'real' and 'negligent' victims, then it would seem wrong to appeal to efficacy here. Did Mr. Carefree's lackadaisical attitude cause his robbery any more than Mr. Stronglocke's hyper-vigilance prevented his? Notice how our intuitions on the case change dramatically if Mr. Stronglocke was also robbed in the story.

The uncertainty about what exactly constitutes an appropriate level of security to meet the NISP should give us pause. If we are unable to identify a clear standard of due diligence, then how can we be expected to consistently judge whether a victim of theft has met her NISP? One thing that should be clear from all of this uncertainty is that it does not follow from either the fact that a burglary occurred or our lack of surprise that Mr. Carefree was the victim that he *deserved* to be robbed. It may be tempting to think that Stronglocke was wise for protecting his property while Carefree was foolish to not better protect his. But even this value judgment does not rise to the level of the belief that Carefree somehow "got what was coming to him." Mr. Carefree does not share in the blame for the burglar (i.e. the burglar is no less to blame for robbing Carefree than he would have been for robbing Stronglocke).

4. Traditional vs. cyber-security

Despite a lifetime of using traditional security measures – the majority of which are strikingly low-tech when compared to the average cyber-security measures – it is difficult (if not impossible) to know with certainty what meeting the NISP actually means. When we consider the technical acumen of the average technology user and the

complicated nature of all that proper computer security entails, one must wonder if it is even plausible to expect the average user to be able to adequately secure their personal data.

Most of us have used some sort of locks and keys for our entire lives and have a rudimentary understanding of how they function and a more robust understanding of how to properly operate them. But, unlike their cyber counterparts, the proper use of a traditional lock requires almost no understanding of the inner workings of a lock. One need not grasp the intricacies of how the pin tumblers inside a lock function in order to know when their lock is locked or unlocked. Most of the things that are equipped with traditional locks are very simple to use and they are reasonably secure when they are locked.

If I buy a padlock to put on my gym locker, I can be reasonably sure that it is ready to use right out of the package. I don't need to run updates or patches to make sure that it functions as advertised over time. There is likely not a lengthy user's manual that I would need to read through in order to understand how to operate it. And it is highly unlikely that the lock will somehow be incompatible with the locker that I want to use it with. Although the lock may eventually break or become worn out from age and overuse, there is no inherent flaw in it that will make it obsolete as other lock technology advances. Ultimately, the fact that I have made the effort to padlock my locker is probably a sufficient deterrent to keep would-be thieves from disturbing the items that I have locked up (it is often said that locks are supposed to keep the honest person honest). Moreover, padlocking one's locker would clearly meet the NISP in most contexts.

Now, let's contrast our simple yet effective (and NISP meeting) padlock with something from the cyber realm, like a wireless router. A Gallup poll from December 2013 showed that 73% of Americans have wireless internet access or wifi in their homes [4]. A study by cyber security specialists at Avast also found that "more than half of all home routers are poorly protected using default or easily hacked password combinations such as admin/admin or admin/password" [5].The reasonable inference from these statistics is that demand for, access to, and use of home wifi has far outpaced either the technical competence or the security consciousness of the average user, or both. This should come as no surprise to anyone who has ever actually installed a home wifi network. The default out-of-the box configuration of most devices is open, unsecured, and aims to facilitate connectivity over security.

Once a network is connected, users typically have dozens of other choices that can help to enhance the security of a home network. But, to the unsophisticated user, much of this probably appears like little more than jargon and technical mumbo-jumbo. What is a firewall and should I enable it? Should my SSID be broadcast (and what is an SSID)? Should I disable wireless admin access or remote admin access or both? Which channels should I use to broadcast? What's the difference between WEP, WPA, WPA-2 and what exactly are bits of encryption? It seems far-fetched to expect the typical wifi user to answer these questions, especially when over half of them don't even have the wherewithal to set up a strong administrator password.

Even if reasonable cyber security stopped at the limits of one's home 802.11 range, that would be enough cause for concern. The good news for hackers is that it doesn't. As devices have become smaller and more portable, mobile on-the-go technology solutions have become ubiquitous. Hackers no longer need to go to the trouble of wardriving to look for unsecured wifi networks, as most users unwittingly bring their unsecured data with them everywhere they go. The December 2013 Gallup poll also revealed that 62% of Americans owned a smartphone (the majority of which now come standard with the offer of some form of cloud based storage). Apple (the industry leader in cloud-based storage) revealed in their January 2013 earnings report that there were over 250 million active iCloud accounts [6]. This shift in where, when, and how we access and store our data has blurred the clearly delineated lines that work so well in our traditional example of home security. Nowadays, it is no longer sufficient to think in terms of locking our digital homes, because anyone with a smartphone, tablet, laptop, MP3 player, ebook reader, or cloud storage potentially takes their virtual home with them everywhere they take their portable devices.

One of the staggering ironies of our increased vulnerability in the cyber realm is that it seems to have been accompanied by a decreased sense of both the nature and severity of the related cyber threat. Many communities throughout the country have Neighborhood Watch programs to patrol areas and provide a deterrent effect against traditional crime. Even the US Department of Homeland Security has instituted a program called "If You See Something, Say Something," with the idea that if everyone is to look out for and report "suspicious activity" then we can all make the country safer [7]. The DHS website lists suspicious activity as including but not limited to:

- *"Unusual Items or Situations"* (e.g., vehicles parked in odd locations unattended packages or other out-of-the-ordinary situations occur),
- *"Eliciting Information"* (e.g., questions at a level beyond mere curiosity – especially about operations or security procedures), and
- *"Observation/Surveillance"* (e.g., paying unusual attention to something beyond a casual or professional interest, loitering without explanation, unusual, repeated, and/or prolonged observation).

While the 'suspicious activity' approach may or may not be effective in combating traditional crime or terrorism, if we apply the same standard to cyber security, it quickly reveals itself as woefully insufficient. Consider the following example. Imagine you see a 'suspicious' person walking through your neighborhood approaching people's homes and turning their doorknobs to see if they are unlocked (for the sake of the comparison, let's grant that the description of 'suspicious' is meaningful and not question-begging). If the suspicious person finds a home that is unlocked, he merely opens the door and peers inside, but he never steals anything, nor even steps across the threshold. Even if he doesn't find any unlocked doors, and thus never actually opens anyone's home without permission, we could still make a strong case that what he is doing is a violation of privacy, and crosses the line of respect for other's property. At the very least, this behavior seems to fit all three of the DHS descriptions of suspicious activity.

Very few of us would consider such behavior acceptable within the present norms governing society. Yet, in the cyber world, this sort of activity is happening constantly. In most cases it occurs without the knowledge of those whose virtual 'doors' are being checked and out of the sight of helpful onlookers who could help by reporting it. The main difference in the cyber world is that the person checking the doors is invisible to most onlookers, capable of checking millions of doors simultaneously, and doesn't have to come to your street to do it – he can do it anonymously from a coffee shop in a country that most Americans probably couldn't find on a map.

The double standard between the real and the digital world not only makes us less secure, it also serves as a sort of tacit consent to the type of virtual door checking described above. If we know that it is happening, yet we do nothing to stop it, then it should not come as a surprise when a twist of the virtual doorknob turns into a full-blown intrusion and theft of data. But, unless we can resolve why the NISP has significantly different traction in analogous cases from the traditional to the cyber worlds, then we can expect that hacking and data theft will be part of a new normal.

5. Human factors and normative standards of security

The foregoing discussion might lead us to wonder whether there can be any normative standard for security. Moreover,if there is some plausible NISP morally pressing on our lives, we must ask if the standard is the same for both traditional and cyber security. Any attempt to define 'an appropriate standard' risks leading us toward a sort of modern-day Euthyphro Dilemma.That is, because we recognize that there is a vital connection between adequate security and effective security, it's tempting to ask whether one's security is adequate because it's effective, or if is one's security is effective because it is adequate? At first glance, this purported dilemma may seem like cause for concern. However, thinking of it as a true dilemma misses the point.

Constructing the problem as a true dilemma with two distinct horns suggests a materially causal relationship between adequacy and efficacy. It suggests that security is adequate if, and only if, it is effective, and that it is effective if, and only if, it is adequate. But it is easy to imagine counterexamples to both horns – suggesting that the dilemma is a false one. For example, Mr. Stronglocke could get robbed and Mr. Carefree may never get robbed, but that doesn't necessarily imply anything about the adequacy of their security. Instead a better way to view security is to consider efficacy as just one component of what makes security adequate rather than as a necessary (and certainly not a sufficient) condition.

A proper normative standard of what adequate security entails (that is, a legitimate NISP) must avoid a broad-brush approach. Adequate security, regardless of the realm in which it is employed, will have some common characteristics. But it is important to differentiate commonality in approach from a one-size-fits-all solution. In the same way that a doctor might prescribe different diets to patients based on genetic predispositions, body

composition, physical activity level, and prior health concerns, so too there should be different prescriptions of appropriate security based on the factors relevant to each case. Whether the goal is to protect collections of coins or collections of ones and zeroes, adequacy depends on the combination of threats and vulnerabilities along with the measures available to respond to them. At the end of the day, the differences between security threats in the traditional and cyber realms disappear when each is approached in terms of threat-based solutions. However, in the real world, given actual human factors in cyber security, the divide remains because the layperson often lacks the insight to properly *adjudicate*a given cyber threat level and/or the knowledge of how to appropriately *respond* to a properly assessed cyber threat.

We contend that the growing disparity in the way that traditional and cyber NISPs are viewed stems not from a fundamental difference in how traditional versus cyber assets are secured, but rather from a confluence of misunderstanding over the vulnerability of electronic data, the threats to those data, and the best way to go about securing vulnerable data. As such, we find that the following criteria should form the basis for a proper normative standard for all security. Note that these are not the typical laundry list of tips that users can implement to make their data more secure. Those lists are excellent and their use is universally highly recommended. But if the only approach to improving cyber security is to increase the demands on users, then the onus also shifts to users as the primary party responsible to prevent crime.

Instead, these criteria recommend the minimum industry standards that should be in place before we look to each individual end user to be responsible for securing their own data.

1. Security solutions should be proportionately affordable to what they are protecting. Just as it wouldn't make sense to buy a very expensive safe to lock up my collection of logo golf balls from all places I travel to, I also don't need a state of the art firewall and intrusion detection system to protect my collection of iTunes library and my collection of cat videos. If I'm protecting my banking data or something else of great value, then it makes sense to consider investing in something which offers a higher level of security.
2. Security solutions should be reasonably easy to employ. Not all cyber solutions will be as simple to use as an old fashioned lock and key. However, the level of computer literacy necessary to use and setup technology should not be vastly different from the level of expertise required to properly secure any data used by that technology. If, for example, a user can setup online banking with a few clicks of a mouse, then there should be a reasonable expectation that adequately securing that user's data against compromise should be just as simple. If, for example, a consumer has an expectation that she will be able to setup her new wifi router through an easy-to-follow GUI, then it is not unreasonable to expect that the manufacturer make securing it just as easy, and a necessary step in the installation of such a device.
3. Use, access, and maintenance of security solutions should provide user convenience without sacrificing security. Investigations following the celebrity photo hacking incident revealed that some of the celebrity's cloud accounts were compromised via the password reminder/question-hint feature designed to help users who may have forgotten their passwords. These systems frequently include questions like "Mother's maiden name," "Street you grew up on," or "name of first pet." Many online services require that users answer several of these as reminder questions part of the signup and registration process. The problem with these systems is that they offer user convenience at the cost of security. A user who takes the precaution of protecting her data connection, using a strong password, and ensuring that her system is up to date and free of vulnerabilities may unwittingly allow intruders access to a backdoor with little more than a cursory check look using a search engine. If a local brick-and-mortar bank or credit union won't let me access someone else's account just because I can tell you that she and "Fluffy" grew up on "Elm St." with her mother, the former Miss "Jones," then I shouldn't be able to do it in the virtual world either.

We believe that before any strong moral judgments can be made regarding the level of complicity or culpability of a victim of cyber theft, the preceding criteria must become the norm. There will always be a difficult balance between convenience and security. Likewise, advances in technology will continue to provide citizens with capabilities that far outpace their ability to secure their data on their own. But, just as locks and keys come standard

on most traditional things that we wish to secure, there should also be reasonable security solutions provided that users are actually able to effectively use without any special expertise.

Lastly, and most importantly, even if users and providers of security solutions do their utmost to prevent data theft, we cannot expect to ever completely eradicate cyber-crime. The best we can do is expect vigilance from all parties involved. But, regardless of the adequacy of security, or lack thereof, it is important to not conflate inadequate security practices with victims deserving to be victimized.

References

[1] CBS Interactive, More Than 100 Celebrities Hacked, Nude Photos Leaked, September 1, 2014, http://www.cbsnews.com/news/jennifer-lawrence-mary-elizabeth-winstead-kate-upton-hacked-dozens-of-nude-photos-leaked/

[2] CBS Interactive, 5 Sony Pictures Films Leak Online After Massive Hack, K. Peterson, December 1, 2014, http://www.cbsnews.com/news/5-sony-pictures-films-leak-online-after-massive-hack/

[3] Priceonomics, The Paparazzi Business, A. Mayyasi, August 8, 2014, http://priceonomics.com/the-paparrazi-business/

[4] Gallup, Americans' Tech Tastes Change With Times, A. Dugan, 2013, http://www.gallup.com/poll/166745/americans-tech-tastes-change-times.aspx

[5] Betanews, Badly Secured Routers Leave 79 Percent Of US Home Networks At Risk Of Attack, I. Barker, November 2014, http://betanews.com/2014/11/05/badly-secured-routers-leave-79-percent-of-us-home-networks-at-risk-of-attack/

[6] Apple Insider, Apple's iCloud Is Most-Used Cloud Service In The US, Beating Dropbox & Amazon, March 21, 2013, http://appleinsider.com/articles/13/03/21/apples-icloud-is-most-used-cloud-service-in-the-us-beating-dropbox-amazon

[7] U.S. Department of Homeland Security, If You See Something, Say Something, https://www.dhs.gov/see-something-say-something