Prying Eyes: What the GCHQ Doesn't Want You To Know

British intelligence has always been tasked with protecting their citizens, and maintaining the overall integrity of the nation. Perhaps that is why some find it so outrageous and ironic that they are the ones infringing upon the privacy of millions. The mass information leak that came from the GCHQ contained incriminating evidence for mass surveillance tactics that were being employed to pry open people's private internet data. These infringements were unannounced, violating to the people, and have not been justified by any counter argument from British Intelligence. If we cannot trust our own governments to protect our privacy, then who ***can*** we trust?

The main focus of organizations such as the GCHQ is to maintain the integrity of public security. Since they are serving and protecting the general population, why would they seek to infringe upon the public? The program has been described as " a breach to our rights to privacy" (Hopkins 2). Other statements released by local police and investigative forces have gone as far to state that the whistleblowers in charge of the surveillance program had "large interest in keeping it private" (Hopkins 3). This admittance of the fact that it was intended to be covered up only strengthens the argument that those in charge knew they were acting immorally. The most frightening part of the whole campaign is that no one can possibly have knowledge of what data is being looked at, or when. There are no official reports or records available to the general public to determine if your content is being searched or not. At this point in time, the only information released is the fact that big-name employees over at the GCHQ have been sanctioning these acts, a secretive violation of "the privacy of millions across the continent" (Gibson 1). As long as British Intelligence

keeps projects like this secret, no one has any way of telling what they might be formulating next.

When you consider it, every byte of data that one posts on the internet is permanent. However, what most people don't know is that even private emails or instant messages can be permanent as well. Sometimes, they can even be accessed by others who are searching for information. Everything that is sent (even 'privately') to another person over the web travels out of the sender's computer, to a hosted online server, which then runs an encryption code to transfer it to the computer of the recipient. Sometimes, the message may be temporarily stored on the site's server until the other user retrieves it. This info can easily be tapped by the average hacker, making it child's play for organizations like the GCHQ. Perhaps part of the reason why they've been conducting their 'data collection' is simply because it is so easy for them. Based on the leak from British Intelligence contractor Edward Snowden, billions of dollars have been invested to "make online privacy obsolete" (Kopczynski 1). Most online services that handle any sort of personal information from their users promise complete secrecy when it comes to that data. It's been shown, however, that the GCHQ has been "maintaining partnerships with the tech companies that provide seemingly secure online communication outlets" (Kopczynski 2). While privacy has been promised over the internet from multiple sources, that does not seem to impede the British Intelligence from conducting surveillance. Human rights to safety and security are not at risk, they've already been compromised, and have been for years.

After all of the information was released, and the GCHQ was made aware that their secret was made public, a formal apology or other form of closure still has yet to be be issued. The organization did not support or warrant their actions. While it's been said that

certain forms of watchfulness "are vital in foreign intelligence gathering and fighting terrorism" (Baldwin 2), the agency itself has not explained their specific reasoning for the covert campaign. It is reasonable that the majority of the public feels lied to and cheated. If a closure statement were to be released, it might help to ease some of the pressure the agency is under at this point, as everyone is demanding answers. Such a statement might also "start the process of re-establishing public trust" (Hopkins 3) that the GCHQ so badly needs at this point. It seems that British Intelligence's role as an aegis would be represented through some type of cogent reiteration of the issue, but no such broadcast has been released so far.

Everything that is posted online is stored somewhere, whether it be a temporary file or a permanent post. Nothing is ever truly deleted, even when it's been deleted from every corner of the internet. It appears that agencies like the GCHQ have latched on to this notion, and are using it to their advantage. Millions across the continent have been affected, whether they know it or not. British Intelligence are always looking out for public safety, but their surveillance campaign across the internet was violating, unjustified, and masked from the public eye. The shameful element of the whole ordeal is that as long as there are users on the internet, programs such as this one will likely continue under command of organizations like the GCHQ, and we will be at the mercy of their authority.

Works Cited:

Hopkins, Nick. "GCHQ Faces Legal Challenge in European Court over Online Privacy." *The Guardian*. Theguardian UK, 3 Oct. 2013. Web. 16 Oct. 2013. <http://www.theguardian.com/uk-news/2013/oct/03/gchq-legal-challenge-europe-privacy-surveillance>.

McDonald-Gibson, Charlotte. "Liberties Groups to Take GCHQ to Court over Web Privacy." *The Independent*. Independent Digital News and Media, 3 Oct. 2013. Web. 16 Oct. 2013. <http://www.independent.co.uk/news/world/europe/liberties-groups-to-take-gchq-to-court-over-web-privacy-8857321.html?origin=internalSearch>.

Kopczynski, Pawel. "Privacy Pulverized: NSA, GCHQ Can Bypass Online Encryption, New Snowden Leak Reveals - RT USA." *Privacy Pulverized: NSA, GCHQ Can Bypass Online Encryption, New Snowden Leak Reveals - RT USA*. RT.com, 5 Oct. 2013. Web. 16 Oct. 2013. <http://rt.com/usa/nsa-gchq-encryption-snowden-478/>.

Balddwin, Caroline. "NSA and GCHQ Unlock Online Privacy Encryption." *NSA and GCHQ Unlock Online Privacy Encryption*. Computer Weekly, 6 Sept. 2013. Web. 16 Oct. 2013. <http://www.computerweekly.com/news/2240204811/NSA-and-GCHQ-unlock-online-privacy-encryption>.