A few connections between Dickinson College, privacy, and security

Thoughts for a "contemporary moment" discussion between Dickinson College students

11/13/2013

Overview: three examples linking Dickinson College to questions about privacy and security. Number 1 is about privacy on the web (think Facebook etc.). Numbers 2 and 3 relate to the Snowden leaks.

1. JenniCam -- check out the Wikipedia page (http://en.wikipedia.org/wiki/Jennicam). While a junior at Dickinson, in 1996, Jennifer Ringley installed a publicly-viewable, almost-always-on webcam in her dorm room (in those days, streaming video was uncommon – in fact, the "webcam" updated with a new static picture every three minutes). JenniCam was mostly uncensored, and apparently it captured some intimate moments, but perhaps the main point was to question the nature of -- and need for -- privacy more generally? Ringley later became a minor celebrity (appeared on Letterman etc.). These days, voyeuristic webcams aren't considered experimental, but it's obviously true that most people are not willing to sacrifice that much privacy. Why? Did JenniCam teach us anything? Is your Facebook page just a milder version of JenniCam?

2. Dennis Blair, Omar Bradley Chair of Strategic Leadership at Dickinson 2007-8, Director of National Intelligence 2009-10. Some reports say Blair was fired by Obama because of his efforts to negotiate a US-France non-spying agreement, which is particularly ironic given the current controversy about US eavesdropping on Merkel's cell phone. (see http://www.nytimes.com/2013/10/25/world/europe/allegation-of-us-spying-on-merkel-puts-obama-at-crossroads.html?smid=pl-share). Should allies spy on each other?

3. Dr Ed Amoroso, Chief Security Officer for AT&T (and Dickinson alum). [Question: how many people think Snowden was right to blow the whistle?] Two weeks ago, Dr. Amoroso came back to Dickinson to give a public seminar about cyber security. And by the way, Dr. Amoroso lives in New Jersey, but immediately after his talk, Dr. Amoroso was driving down towards Washington DC – why? To visit the NSA. He didn't reveal any details about what he would be discussing there, but we can guess some aspects of it. The main thrust of his talk was a fascinating perspective on the history of cyber security, and he didn't address the Snowden leaks directly. But it became clear from one or two comments that Dr. Amoroso believed Snowden was wrong to leak the documents. It's interesting to think about this from the point of view of someone who works at a senior level in a communications company. Clearly, AT&T was forced to comply with legal orders from NSA etc resulting in some form of spying on people. In addition, there have been some more recent revelations about AT&T being paid by the CIA for data about calls (about than five days ago, see http://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html?smid=pl-share). Obviously, I'm picking on AT&T here, purely because of the Dickinson connection. Because of the Snowden leaks, we know that many other companies have

cooperated with some form of governmental spying. What are we giving up when this happens? What are we gaining? One final comment, which was actually a very interesting point made by Dr. Amoroso himself during his talk: has anyone actually sent or received an encrypted e-mail recently? Anyone use Gmail? Wouldn't you think Google is capable of encrypting your e-mails? Unfortunately, that would break their business model. Google needs to be able to read your mail in order to show you targeted ads! So, perhaps this is an example of commercial interests trumping privacy and security. Can we expect this to be a lasting feature of online services?