Cyber Matters

1: Introduction

Hi, and welcome to this first post of what will become my capstone project for the misleadingly boringly named PUBPOL 290-02, Intro to Cyber Policy. What follows will be a collection of thoughts, written in casual style and readable prose, on the state of cyber policy and security here in the U.S. and worldwide. I'm writing this for this particular course, but I'd like it to be broadly readable and interesting, even to people who haven't spent the semester thinking about the state of cyber—if this describes you, please do keep reading! I'm going to write with the assumption that my readers aren't experts on cyber-security and I'll try not to bore you with background information if it's not necessary. In terms of content, I'll talk about some problems I see for the average human as they go about their daily lives in our not-so-tech-savvy world, how serious those problems might or might not be, and some ways I would go about trying to fix them, if for some horrifying reason that were my responsibility. Being a computer science guy, I'll also work my way through a few proofs of concept (or perhaps it would be more accurate to say "exuberant defenses of concept") for technical tools that, if implemented by someone far more talented and experienced than I, might do some real good for collective cyber-health and happiness. If I'm lucky, I'll have a prototype to share with you all as well.

But first, a little about my philosophy on cyber as a field and the issues surrounding it. I'm a strong believer that cyber issues are human issues. That is, I believe that problems which arise from the world of the internet, or from technology more generally, stem from the same problems that humans have been trying to deal with since the dawn of time: allocating resources, balancing privacy and security, respecting cultural differences, staying healthy and sane, etc. Take, for example, the recent Capital One data breach, which leaked the credit card applications of over 100 million users. On one hand, the attack was a complex theft requiring advanced technical knowledge of how firewalls should be configured between Amazon Web Services (AWS) and a client application (Capital One's). On the other, though, it was a tale as old as time: an employee who knows her company's product inside-and-out gets fired, gets angry, and decides to see what she can do to get back at her former employer. Realistically, it's difficult to say how we could ever fully protect against this kind of attack without preventing people from getting angry, which I would call, in a possible understatement, impossible.

We've talked a lot in this class about "reasonable hope" in the context of cybersecurity. It's easy to get overwhelmed by all of the cyberthreats out there: identity theft, fraud, cyber warfare, harrassment, and a whole host of others. Is privacy dead? Is all of our data being stored on the black market? Often what helps to ground oneself and hold oneself steady against all of this uncertainty is to ask: what's the reasonable hope here? For me, this hope comes from a trust that where we humans create problems, we can also solve them, and since cyber issues are in fact human issues, I trust that we can work through those too. Call me blindly optimistic, call me naive, but I truly believe that. What it will take, though, is some real thought and work from all of us, from humanity. We have to decide what kind of society we want to live in and exactly which elements of the cyberspace are worth having with us into the future. It can't just be tech people who decide either. We have to involve as much of the world as we can in discussion and thought and policy-making and engineering.

Now, let me chill out with the grandiosity (before I inadvertantly submit my name as a Democratic presedential nominee) and get on to the good stuff.