Application for Review of Human Research: IRB Protocol Summary
Social and Behavioral Sciences

Section II
[Ver 1 3.4.2011]

Principal Investigator: John Smith

PROTOCOL TITLE: Fast Times in InfoSec: A Study of Speeding Among IT Security Staff and Their Children

STUDY SPONSORSHIP
1. Funding Sponsor: The University of Pennsylvania and the University of Albany.

INTRODUCTION AND PURPOSE
The purpose of this study is to examine speeding habits of risk averse IT Security Staff and their children. Starting from the premise that risk compensation will lead IT Security Staff to acquire safer cars and therefore speed more often, we will acquire quantitative GPS-based data about the frequency and degree of speeding among IT Security Staff. As a secondary measure we will compare their speeding habits to the habits of their children of driving age.

In addition, we will study the correlation between speeding and other risky behaviors by asking subjects to complete an on-line survey about past and present risk behaviors including illegal drug use, criminal records, and the riskiest actions they’ve ever taken at work.

Finally, to study the amplifying effects of social interaction on risky behavior, we will ask subjects to identify their LinkedIn “connections” whom they believe to be most likely to speed or engage in risky behavior. We will then contact these LinkedIn individuals, and ask them to participate in the study, as well.

OBJECTIVE:

CHARACTERISTICS OF THE STUDY POPULATION

1. Target Population and Accrual
100 IT professionals will be selected from major universities near Philadelphia and New York.

2. Key Inclusion Criteria
   ● Only IT professionals will be included in the study.

3. Key Exclusion Criteria
   ● Non-IT professionals

4. Subject Recruitment and Screening
All subscribers to the Educause Security List will be contacted and asked to participate in this study. Additional subjects (from LinkedOn connections) will be accrued using snowball sampling. University IT contact information will be harvested from public directories to find contact information.

5. Early Withdrawal of Subjects
Subject can withdraw at any time by contacting the researchers.

STUDY DESIGN

Participants will be asked to allow a GPS device to be installed in their cars. Over one month, this data will be collected by GPS-maker Carmint. The data will be uploaded to a secure web application run by Carmint. We will download the data nightly to a dedicated, password-protected computer in our lab.

After the first month of data collection we will ask that they install the device in the car most frequently driven by their children. We will then collect a month of this speeding data in order to compare habits of parents and children.

In the second part of the study, participants will be asked to complete a survey about risky behaviors using SurveyGorilla. Questions will include detailed measures of frequency, past and present, of illegal drug use, criminal records, and riskiest actions taken at work. This data will be downloaded from SurveyGorilla at the end of the 2 week survey period onto a secure, password-protected computer in our lab.

Finally, subjects will be asked to identify other participants for this study by choosing their LinkedOn connections that they think are most likely to speed, take drugs, or commit crimes. They will submit these to us by sending email to FastTimes@gmail.com with their connections’ name, email address, and LinkedOn username. We will contact these LinkedOn users through LinkedOn, and will build out the network based on 2nd and 3rd level connections.

5. Data Management
Data will be stored on password-protected computers and all files will be encrypted.

STUDY PROCEDURES

4. Statistical Analysis
Surveys will be analyzed using SPSS. GPS data will be linked to survey results.

RISK/BENEFIT ASSESSMENT

1. Risks
Risk are greater than everyday life. Participant GPS data will most likely contain evidence of speeding and the surveys may contain evidence of illegal drug use or compromising behavior at work. Also, there is a risk of breach of confidentiality. These risks are minimized by limiting access to protected computers to only research staff. All data will be anonymized after data collection is complete.

2. Benefits
Participants will not receive benefits.

3. Subject Confidentiality
Confidentiality is protected by using password protected computers using 128-bit encryption.
How will confidentiality of data be maintained? Check all that apply.

- Computer-based files will only be made available to personnel involved in the study through the use of access privileges and passwords.
- Prior to access to any study-related information, personnel will be required to sign statements agreeing to protect the security and confidentiality of identifiable information.
- Whenever feasible, identifiers will be removed from study-related information. A Certificate of Confidentiality will be obtained, because the research could place the subject at risk of criminal or civil liability or cause damage to the subject’s financial standing, employability, or liability.
- Precautions are in place to ensure the data is secure by using passwords and encryption, because the research involves web-based surveys.

INFORMED CONSENT

1. Consent Process

Written consent is being obtained.