Project Ideas

Analyzing the business relationship of new ad programs: Tracker blocking tools such as AdBlock Plus and Brave allow acceptable ad programs. However, the business relationship between these tools and advertisers is unknown. The purpose of this project is to shed light into this hidden business relationship. Doing so means looking at domains that are serving ads in the presence of these tracker blocking tools.

Ad-free alternative web browsing experience: We frequently experience unwanted ads while browsing the web. While some sites provide the option of ad-free paid subscription, such paid subscription scheme has not received wide adoption. The purpose of this project is to explore other alternatives that are more likely to be adopted by users. Such alternatives may include crowdsourcing based micropayments (Brave browser has an Ad reward program). Student will be expected to design a study to understand if any such alternative would not only be feasible, but also acceptable to end users. This project will require IRB approval, so work on this early.

Tracking ecosystem in desktop vs. mobile platforms: There has been extensive web measurement for determining the prevalence of trackers. However, most of the measurements have been done in the context of desktop platform. The goal of this project is to determine if there is a difference in tracking behavior for mobile platform when compared to desktop platform. Students will be expected to carry out large-scale data collection using some form of automated web measurement framework.

Usability of privacy enhancing tools: Users have started using various privacy enhancing tools nowadays, including browser extensions such as adblock+, Ghostery, Disconnect and Tor. But why do people use such tools? What are the main concerns for using such tools? Are people mostly concerned about the ads or the tracking? How effective are these tools at detecting ads or tracking? What websites break when people use these tools? Students working on this project would conduct a survey to understand users' mental model for using privacy enhancing tools. This project will require IRB approval, so work on this early.

Holistic analysis of tracker-blocking tools across platforms: Compare the effectiveness of different privacy enhancing web tools like adblock+, Ghostery, Disconnect and Tor across different platforms (like desktop vs. mobile). Study their default settings. Study user expectations under default configurations.

Web measurement study: Analyzing the impact of GDPR on websites: Conduct a web measurement study that provides insights into the prevalence of trackers on web sites. Students can use web-measurement frameworks such as OpenWPM and other privacy tools such as Ghostery to measure the presence of various trackers on sites. The study should also look at how the distribution of trackers loaded on various sites vary across different geographic locations (e.g., US vs. EU).

Compliance of privacy policies with GDPR: With the rise of new regulations such as EU's GDPR, industries need to provide users with explicit privacy notices regarding the collection of any personal data. GDRP also mandates providing users with options to modify, delete and even export their data. This project will involve closely looking at the privacy policies of popular Internet of Things (IoT) products/services (e.g., Amazon echo, Nest Thermostat) to verify whether they comply with GDPR.

Privacy notice for wearable and Internet of Things (IoT) devices: While standardized privacy notice formats exist for various domains, for example privacy nutrition labels for websites and Gramm-Leach-Bliley Act [GLBA] privacy notice requirements for financial institutions, wearable and IoT devices pose a unique privacy challenge due to their continuous data collection and close proximity to user's physical body. The goal of this project is to design and evaluate a standardized notice format for wearable and IoT devices. This includes identifying what users care about and what is the best way to notify such information to users (see A Design Space for Effective Privacy Notices to get started). This project will require IRB approval, so work on this early.

Privacy oracle: Providing users with privacy-related advice: Most of the times users have many questions about how their data is collected and how they can control what information is collected about themselves. However, often they don't know how to enforce privacy choices in spite of privacy settings at times being present. This project will involve designing a user study (or interview) to ask users about what privacy related questions they traditionally have and how they would want to seek answers. The project should layout the design of a system that users can consult to seek privacy-related advice. This project will require IRB approval, so work on this early.

Ethical use of AI to make privacy-related decisions: With the rise of employing AI or machine learning techniques to automate many of our decision making, there is a growing concern about whether such techniques are making the best decisions. This project will involve designing a user study to evaluate how people feel about the use of AI or machine learning techniques to make automated decisions (e.g., automated cars or AI-powered mortgage lender). This project will require IRB approval, so work on this early.

Privacy concerns of using facial recognition based systems: In recent years we have seen the rise of using facial recognition based systems for commercial applications. Examples include restaurant menu suggestion, automated check-in and check-out, and determining interest based on facial expression. However, it is unclear to what extent people are comfortable with these services automatically collecting, analyzing or even sharing our facial data. This project involves understanding how people feel about the use of facial recognition based systems..

Privacy concerns with embracing smart cities: In recent years, we are seeing a push towards deploying smart infrastructures to build smart cities. The goal of this project is to understand how users feel about embracing such data-driven smart environments. This may include answering questions such as do users have any privacy concerns, if so what are those concerns? Are they willing to compromise personal data to embrace the benefits of smart cities? What form of data transparency would they like to see, if any? This project will require IRB approval, so work on this early.

How accurate is your online profiling?: It is well-known that users are tracked across websites for behavioral advertising. However, little is known about the accuracy of these profiles? The goal of this project is to understand how users feel about the online profiles that are created based on their browsing habits. Students can use profile transparency pages such as Google's Ad Settings and bluekai Registry for this purpose. Students need to design a study where they will ask users to review such transparency pages and collect their impressions (e.g., whether they are surprised or shocked).

Privacy implications of using smart voice assistants: In recent years we have seen a steady growth of smart voice assistants like Amazon Alexa. However, it is not clear to what extent these services use our voice commands to create behavioral profiles. The goal of this project is to analyze if voice commands are used to create behavioral profiles, and if such profiles are visible through ads on other platforms (e.g., on mobile phones or laptops). Students would interact with a smart voice assistant mimicking various controlled behavioral profiles and then correlate ads or search engine recommendations with corresponding behavioral profiles.

Information leak in automation tools or services: With the rise of Internet of Things we have now started seeing automation services such as Zapier, IFTTT and Microsoft Flow be widely used. However, such automation rules may leak sensitive information which users may not realize when setting up such rules. The purpose of this project is to design/prototype a tool or service that users can utilize to better understand the security and privacy implications of setting up vulnerable automation rules.

Infer high-level human activity from network traffic: The goal of this project is to infer high-level human activities that take place in a smart home by only looking at encrypted network traffic. You will use ML techniques to detect patterns to infer high-level activities. We have an IoTLab for collecting such data.

Generating data-provenance graph from IoT traffic: The goal of this task will be to look at network traffic generated by different IoT devices to generate a data-provenance graph. The graph will enable us to potentially determine business relationships among different vendors.

Analyzing Alexa skills: The goal of this project is to build an automated system that can intelligently interact with Alexa skills and record (voice-to-text) all the interactions for further analysis. Such analysis would include whether the skill is performing what it is claiming on the skill store page or whether the permissions requested by the skills make sense.

Providing privacy notice using virtual reality technology: Exploring if VR or AR technology can be used to help users become more aware of different privacy implications and thereby make better privacy decisions. This would potentially be a user study (crowdsourcing task) where users would interact with VR/AR technology and provide feedback.

Privacy concerns in adopting IoT across people from different culture/country: The goal of this project will be to do a user study to determine the different factors that influence users to buy or use emerging IoT technologies. What factors influence their buying habits? What are their main concerns? Or what are the concerns of people near them?