CS60055: Ubiquitous Computing

Ethical Aspects of UbiComp

Department of Computer Science and Engineering

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Sandip Chakraborty
sandipc@cse.iitkgp.ac.in

Privacy Invasion

- **Data Collection**: Needs constant data collection from sensors, devices, and networks to provide personalized experiences
  - leads to extensive collection of personal and often sensitive data (e.g., location, health metrics, behavioral patterns)

- **Lack of Transparency**: People may not be fully aware of what data is being collected, how it's used, or who has access to it
  - Raises concerns about consent and informed participation

- **Surveillance**: Ubicomp can facilitate mass surveillance by corporations, governments, or even individuals
  - Potential infringing on individual freedoms and autonomy

Privacy Invasion: Multiple Research Works in the Past Decade

Privacy Leakage via Speech-induced Vibrations on Room Objects through Remote Sensing based on Phased-MIMO

Cong Shi, Rutgers University, cs1421@scarletmail.rutgers.edu
Tianfang Zhang, Rutgers University, tz203@scarletmail.rutgers.edu
Zhaoyi Xu, Rutgers University, zx111@soe.rutgers.edu
Shuping Li, Rutgers University, sl1567@scarletmail.rutgers.edu
Donglin Gao, Rutgers University, dg921@soe.rutgers.edu
Changming Li, Rutgers University, cl1361@scarletmail.rutgers.edu
Athina Petropulu, Rutgers University, athinap@soe.rutgers.edu
Chung-Tse Michael Wu, Rutgers University, ctm.wu@rutgers.edu
Yingying Chen, Rutgers University, yingche@scarletmail.rutgers.edu

mmEve: Eavesdropping on Smartphone's Earpiece via COTS mmWave Device

Chao Wang[1,2], Feng Lin[1,2*], Tiantian Liu[1,2], Kaidi Zheng[1,2], Zhibo Wang[1,2], Zhengxiong Li[3], Ming-Chun Huang[4], Wenyao Xu[5], Kui Ren[1,2]
[1]Zhejiang University, Hangzhou, China
[2]ZJU-Hangzhou Global Scientific and Technological Innovation Center, Hangzhou, China
[3]University of Colorado Denver, Denver, Colorado, USA
[4]Duke Kunshan University, Kunshan, China
[5]SUNY Buffalo, Buffalo, New York, USA

Acoustic Eavesdropping through Wireless Vibrometry

Teng Wei[†], Shu Wang[†], Anfu Zhou[*†] and Xinyu Zhang[†]
[†]University of Wisconsin - Madison, [*]Institute of Computing Technology, Chinese Academy of Sciences
{twei7, swang367, azhou9}@wisc.edu, xyzhang@ece.wisc.edu

Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting

Tao Ni, *Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong;* Guohao Lan, *Department of Software Technology, Delft University of Technology;* Jia Wang, *College of Computer Science and Software Engineering, Shenzhen University;* Qingchuan Zhao, *Department of Computer Science, City University of Hong Kong;* Weitao Xu, *Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong*

Security Risks

- **Vulnerable Devices**: Many IoT (Internet of Things) devices have limited security protections

- **Unauthorized Access**: Ubiquitous systems often operate without explicit user intervention

Check Point experts discovered a high-severity flaw in Philips Hue Smart Light Bulbs that can be exploited to gain entry into a targeted WiFi network.

Security experts from Check Point discovered a high-severity flaw (**CVE-2020-6007**) in Philips Hue Smart Light Bulbs that can be exploited by hackers to gain entry into a targeted WiFi network.

Lightbulbs could be remotely controlled through a mobile app or via a digital home assistant, owners could control the light in the environment and even calibrate the color of each lightbulb. Smart lightbulbs are managed over the air via WiFi protocol or ZigBee, a low bandwidth radio protocol.

Autonomy and Consent

- **Lack of Control**: Individuals might have limited control over the devices and systems operating around them
  - Leads to decisions and actions that may affect them without their consent
- **Implicit Consent**: Many systems rely on implicit consent, where people are assumed to agree to data collection simply by being in a location with pervasive sensors
  - Makes it difficult for users to opt out or avoid these systems
- **Manipulation**: With access to behavioral data and predictive algorithms, companies can tailor experiences in ways that subtly manipulate user behavior (e.g., targeted advertising)
  - Potential infringing on an individual's autonomy

Surveillance and Tracking

- **Constant Monitoring**: The continuous tracking of location, behavior, and interactions can lead to a surveillance society
  - People's movements and actions are always monitored
- **Chilling Effect**: Knowing that one is being monitored can lead to self-censorship and a reduction in personal freedom
  - People might alter their behavior when they know they're being tracked
- **Social Sorting**: Data collected by ubiquitous systems can be used to categorize people
  - Leads to profiling -> may influence access to services, employment, or other opportunities -> leads to discrimination

Bias and Discrimination

- **Algorithmic Bias**: Often rely on algorithms that may be biased based on the data they are trained on, leading to unfair treatment of certain groups

- **Unequal Access and Digital Divide**: Not everyone has equal access to technology, creating disparities in who benefits from ubiquitous computing.
  - Could reinforce social inequality, especially if essential services become embedded within such systems

- **Data-driven discrimination**: Profiling based on collected data may lead to discriminatory practices
  - Behavioral patterns, emotional states, etc. Are extremely sensitive information

Informed Consent and User Understanding

- **Complexity and Comprehension**: Challenging for users to fully understand how they work and the implications of interacting with them
  - Lack of comprehension makes true informed consent difficult
  - **Example:** What would be the best way to collect emotion data from individuals?

- **Hidden Data Flows**: Users may not realize the full extent of how their data is shared across platforms, devices, and third-party services
  - Makes it harder to control or withdraw consent

Environmental Impact

- **E-Waste**: The proliferation of sensors and connected devices increases electronic waste
  - These devices often have short lifespans and are hard to recycle.

- **Energy Consumption**: Continuous data collection, processing, and connectivity require significant energy
  - Contributes to a larger carbon footprint.

Ethics of Data Ownership and Rights

- **Ownership of Personal Data**: As ubiquitous computing collects massive amounts of personal data, questions arise about who owns this data and who should benefit from it.

- **Right to be Forgotten (RTBF)**: Individuals may want to erase past data, but in a highly interconnected system, implementing this can be challenging

- **Data Monetization**: Companies often profit from personal data
  - Raises ethical concerns about the commodification of individual behavior and preferences without fair compensation

Addressing Ethical Concerns

- **Privacy by Design**: Integrate privacy protections into the design of systems from the outset, rather than as an afterthought.
- **Transparency and User Control**: Offer users clear explanations of data collection practices and give them control over what is collected, shared, and retained.
- **Robust Security Practices**: Implement strong security measures to protect data, including encryption, authentication, and regular security audits.
- **Algorithmic Fairness**: Regularly test and refine algorithms to ensure they don’t exhibit bias or lead to discriminatory practices.
- **Sustainable Practices**: Design devices and systems with sustainability in mind to minimize environmental impact.

Ethical Criteria for Human Data Collection

- **Informed Consent and Transparency**
  - **Clear Consent**: Obtain explicit consent from participants, explaining what data will be collected, how it will be used, who will access it, and any associated risks.
  - **Transparency**: Ensure that users understand what data is being collected, why it's necessary, and how it benefits them. This includes detailing third-party data sharing or analysis practices.
  - **Easy Opt-Out**: Allow users to withdraw consent and opt out at any point, with clear instructions on how to do so.

Ethical Criteria for Human Data Collection

- **Data Minimization and Relevance**
  - **Only Collect Essential Data**: Collect only the data necessary to fulfill the purpose of the project, avoiding excessive or irrelevant data collection.
  - **Purpose Specification**: Define clear, specific purposes for data collection and ensure that all data aligns with these objectives.
  - **Contextual Relevance**: Consider the context in which data is collected to ensure it is relevant to the project's goals. For example, tracking location may be relevant for navigation aids but intrusive for other applications

Ethical Criteria for Human Data Collection

- **Privacy and Anonymization**
  - **Anonymization and Pseudonymization**: Whenever possible, anonymize or pseudonymize data to protect user identities.
    - This involves removing *personally identifiable information* (PII) that could be used to trace data back to individuals.
  - **Data Aggregation**: Use aggregated data rather than individual data points to provide insights while reducing the risk of privacy invasion.
  - **Data Access Controls**: Implement strict access controls so only authorized personnel or systems can view sensitive data.

Ethical Criteria for Human Data Collection

- **Data Security and Protection**
  - **Secure Storage**: Store data securely using encryption, both in transit and at rest, to prevent unauthorized access and data breaches.
  - **Robust Authentication**: Use multi-factor authentication and other security protocols to protect access to the data.
  - **Data Retention Policies**: Establish and communicate clear data retention policies to ensure data is not stored indefinitely and is deleted when no longer needed.

Ethical Criteria for Human Data Collection

- **Fairness and Bias Mitigation**
  - **Bias Check**: Regularly check for and address biases in data collection and analysis to prevent discrimination or unfair treatment of certain groups
    - The inclusion/exclusion criteria needs to be defined clearly
  - **Diversity in Data**: Ensure the data collected represents a diverse user base to avoid skewed outcomes that may not generalize well across different populations.
  - **Algorithmic Fairness**: Design algorithms and models to treat all individuals equitably
    - Take measures to avoid perpetuating or amplifying biases in the data.

Ethical Criteria for Human Data Collection

- **Data Accuracy and Quality**
  - **Ensure Data Quality**: Collect high-quality, accurate data that reflects real-world scenarios relevant to the project.
    - It might be sometime confusing to define what is "accurate"!
  - **Validation and Verification**: Implement validation techniques to ensure the accuracy of the data being collected and to detect errors or anomalies.
  - **Data Update Mechanisms**: In applications where data can quickly become outdated, such as location or health data, establish mechanisms for regular updates to maintain accuracy.

Ethical Criteria for Human Data Collection

- **Ethical and Social Responsibility**
  - **Ethical Impact Assessment**: Assess the ethical implications of data collection, especially if it involves sensitive information like health, financial, or behavioral data.
  - **Avoid Harmful Uses**: Ensure that data collection and usage do not cause harm, misuse, or exploitation of participants, either directly or indirectly.
  - **Respect for Context**: Be sensitive to the context in which data is collected and used.
    - For example, data collected in private or personal settings should be treated with extra care

Ethical Criteria for Human Data Collection

- **Transparency in Data Use and Sharing**
  - **Usage Transparency**: Inform users about how their data will be used and analyzed, including any AI or machine learning applications that might affect their experience.
  - **Third-Party Sharing**: Clearly state if data will be shared with third parties, the purposes of sharing, and how it will be protected.
  - **Data Lifecycle Disclosure**: Explain the full lifecycle of the data, including collection, storage, usage, sharing, and eventual deletion.

Ethical Criteria for Human Data Collection

- **Compliance with Legal and Regulatory Standards**
  - **GDPR, CCPA, and Other Regulations**: Adhere to privacy regulations such as the General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA), or other regional standards.
  - **Data Protection Officer (DPO)**: In projects involving large-scale data collection, appoint a Data Protection Officer (DPO) or similar role to oversee data practices and ensure regulatory compliance.
  - **Ethics Board Approval**: For sensitive or potentially controversial projects, seek approval from an ethics board or committee to ensure that the project aligns with legal and ethical standards.

Self-Read

- General Data Protection Regulation (GDPR): https://gdpr-info.eu/
- Edyta Bogucka, Marios Constantinides, Sanja Šćepanović, Daniele Quercia (Nokia Bell Labs Cambridge), "Co-designing an AI Impact Assessment Report Template with AI Practitioners and AI Compliance Experts", Vol. 7 (2024): Proceedings of the Seventh AAAI/ACM Conference on AI, Ethics, and Society (AIES-24) : https://ojs.aaai.org/index.php/AIES/article/view/31627/33794


Happy
Learning!