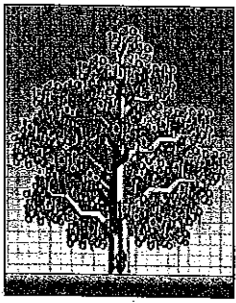
Editor: Munindar P. Singh • m.singh@ieee.org

Privacy Risks in Intelligent User Interfaces



Christopher J. Hazard • *Hazardous Software*

Munindar P. Singh • *North Carolina State University*

Intelligent user interfaces (in games, for example) provide opportunities for producing a high-quality, contextually relevant user experience. However, they also raise the specter of privacy violations. The authors review some of the ways in which user interfaces could glean a user's private information; then the authors highlight the risks therein, and discuss ways of mitigating those risks.

We define an *intelligent user interface* or IUI as (part of) an app that interacts with a user in a way that's responsive to the user's changing needs at the time of interaction. That is, an IUI provides functionality in a way that is adaptive to specific users and to their specific contexts of usage, as those contexts arise and change in the field. Typically, an IUI would construct and maintain a model of the user and the user's context. As part of doing so, an IUI would capture relevant aspects of the user's profile (possibly including demographic information), interaction and communication history, goals, preferences, social relationships, traits such as personality, and physiological and psychological states. Not every IUI needs all these aspects, but depending upon the underlying purpose of the app and how ambitious its designers are, an IUI might capture more or fewer of them.

Examples of IUIs include tools that support calendars and navigation (such as Google Now); dialogue apps (such as Apple's Siri); and games — both those on fixed devices and those that are inherently mobile (such as Pokémon Go).

IUIs can function effectively only because of the information they collect or access about each user. Some information might be provided by any of the following:

- directly from the user (such as your age and sex);
- user-allowed access to other services (such as your email content, friend lists, and such);
- explicit interactions with the user (such as through your prior queries and their results);
- data implicitly gathered about the user (such as from the locations you visited or the locations where you played a particular game);
- explicit requests from the IUI (for example, if it asks whether you would like to receive this call); and
- inferred user interactions (such as your preference for less-interactive content during the morning and late at night).

Armed with this information, an IUI seeks to offer an enhanced user experience by figuring out the user's goals and preferences and acting accordingly.

Under weak assumptions of how users behave or by learning such patterns across the entire body of users, an IUI can figure out additional details about a user that the user might never have realized were being revealed. For example, it isn't farfetched to guess that a user's home or work is one of the locations at which a user is most frequently present or one of the origin locations from where the user most often searches for routes to other locations.[1] In addition, users (even those who work and live in the same locations) would have mutually distinct trajectories on a day-to-day basis — thus, users' trajectories can serve as pseudonyms for them.

Increasingly, privacy is recognized as a major concern. The privacy risks of games have received public and congressional attention (see www.franken.senate.gov/files/letter/160712_PokemonGO.

2469-7087/17/$33.00 © 2017 IEEE

pdf). As IUIs collect more types and amounts of data on users, the associated risk of disclosure increases. Moreover, privacy is more than a concern about access to information; it includes considerations such as infringement on a person's autonomy, intrusion into private space, and loss of dignity.[2] A proper understanding of privacy not only can help us reduce avoidable risks, but by doing so, also reduce the so-called "chilling effect" of government or corporate surveillance on people's behaviors, and thereby enhance the potential individual and societal value of modern intelligent apps.

Why IUIs Are on the Rise: Potential Benefits

IUIs are expanding because they're valuable. As the available information and decisions grow, there's an increasing need to select appropriately among them. In addition, user time, attention, and effort are increasingly at a premium as information technology is deployed in more and more natural settings, not merely in your office. As a result, users do need greater support in their decision making, and such support must accommodate the user's needs by taking into account a rich model of the user.

In simple terms, what IUIs offer is intelligent discrimination between numerous raw possibilities to select actions that best capture a user's goals. For example, if the authors (based in Raleigh, North Carolina) are looking for an address in Durham, they more likely mean Durham, North Carolina and not Durham, United Kingdom. A navigation app that automatically chooses the nearby Durham can do so only if it knows where the requestor is based. We wonder if an IUI would have helped avoid the error that led a Belgian woman on a 3,000 km off-course drive.[3]

The problem requires greater intelligence than fixed rules, however. For example, if an email indicates an airline ticket booked to Tees Valley Airport, then maybe it's the UK's Durham that's salient, though with the origin set to Tees Valley Airport.

Likewise, a game or an educational app might choose between challenges to present to a user based on how tired or competent the user is – better players or students get harder challenges so they won't be bored and others get simpler challenges so they won't be frustrated. This is nothing but an application of Mihaly Csikszentmihalyi's[4] idea of the flow channel, and is a commonplace tenet in game design.[5] Of course, to support such functionality presupposes determining how competent, tired, or anxious the user is.

Privacy Risks

In a nutshell, IUIs bring forth the following tension: To operate effectively, they need to acquire or construct rich information about the user. The most valuable of such information is potentially sensitive and revealing; it can pose a threat to the user's safety, finances, or dignity (just imagine if it becomes known that you're the slowest student in your class).

Privacy risks arise in a variety of settings. For example, if you stored a "home" location on your navigation app on your phone, a criminal who steals your phone can then navigate to your home as well to rob or attack you. We don't emphasize such risks in this article, because they rely upon an external attack on an IUI or a device. Instead, we primarily consider risks where the attack is through the app itself. An example of such an attack would be where your navigation app routes you by an ice cream shop or a pub on your way home, based on the assumption that a subtle suggestion (when you're tired at the end of a long day of walking or driving) might cause you to visit such an establishment.

Extracting and Disseminating Information

Information can be extracted from machine learning models that have been trained, even if the original data isn't accessible.[6] Such models function as a form of data compression of a subset of the user's private data, capturing the nuggets of information that are potentially most sensitive for the user. In many cases, the user might not have known that sensitive data was being collected, because it's hidden within routine data, but machine learning brings it forward. For example, consider an IUI that learns a user's preferences over time for the purpose of improving user productivity. In this example, the IUI might learn artifacts about the user that aren't explicitly related to the task, such as the time that the user wakes up in the morning or what times of day the user isn't productive. Neither the user nor the app developer might have realized that this information was contained within the learned data.

If the IUI were to disclose such sensitive information to others, that would be a privacy risk. For example, if your calendar informed your boss that you began work not at 8:00 a.m. but at 10:00 a.m., that might be significant. The outcome might be just as harmful if the calendar informed your clients that you were available at 8:00 a.m. but not ready to talk to them, simply because you were reserving the time for "more important" tasks.

Probing Users

An IUI doesn't merely have to passively observe a user; it can actively probe a user by presenting carefully chosen alternatives to a user as a way to learn about the user's physiological or psychological state. From the choices the user makes, an IUI can potentially infer information about whether the user is depressed[7] or dieting,[8] and can estimate other psychographic measures related to decision fatigue. Recent work has suggested that decision fatigue and ego depletion may be at least somewhat specious[9] (or at least not reliably reproducible), calling some question on the validity of some previous studies. However, a widely deployed app that performs empirical analysis doesn't have to work in general, only in its particular setting. Such an app can quickly gather actionable empirical results far larger than academic studies, possibly incentivizing the developer to keep the data proprietary for commercial gain. If an IUI can, in some way, utilize some aspect of decision fatigue, the user can be controlled in unusual ways.

Compromising Security and Identity

Many authentication protocols rely upon bringing out shared secrets. For example, credit card transactions often require stating the customer's home address to corroborate that the customer is legitimate. And, when a situation raises some red flags, credit card companies ask users to verify which transactions they carried out at which sites – presuming that only the genuine user would know of them. But a location-based app might be able to guess your home address as well as brick-and-mortar establishments you've visited where you might have made purchases. So a rogue IUI can easily help compromise your security and identity.

Directly Manipulating Autonomy

We define *direct manipulation of autonomy* as partial or total control over a user's actions characterized by a moderate to high probability of success for any given interaction. In other words, it's likely that a user experiencing this form of manipulation will have a high likelihood of being coerced into doing something they otherwise wouldn't have done. These types of manipulations might or might not require private information to work, but they might be enhanced by private data or personally identifiable information (better known as PII) and they could yield private data or PII.

Dark patterns, wherein a user interface is crafted to trick users into performing a particular task, are instances of attacks that directly manipulate autonomy (see http://darkpatterns.org). An example of a dark pattern is a navigation app that repeatedly asks, until you agree, if you would like to permanently allow the service provider to collect detailed data from your phone to improve your results. By frustrating the user enough, such an app in effect coerces the user to agree after a few episodes: subsequently, the user might forget having granted this permission or be unable to find a way to rescind the permission.

Indirectly Manipulating Autonomy

We define *indirect manipulation of autonomy* as partial control over a user's actions, characterized by an extremely low probability of success in manipulation at any given interaction. In other words, a successful manipulation either requires exposure to a large audience, numerous exposures to the same user, or both.

Examples of indirect manipulation of autonomy are advertisements, layouts of interfaces, hardware, or other interactions that yield slight differences in behavior in aggregation. Changes in interfaces, for example, relate to what's called *choice architecture,*[10] where the choices being encouraged are given prominence or made easier. For example, many casual games have in-game purchases that allow the player to advance more quickly through difficult or frustrating parts of the game. The game developer can present the player the option to purchase an item that will increase the chances of speeding through the difficult section at the most opportune times. By gathering data en masse about players, various analytical techniques can indicate when players are most likely to make a purchase and how to improve retention when players are about to stop playing the game, enabling developers to capitalize on these tendencies.

Aggregate data about individuals can drive indirect manipulation of autonomy by giving those who employ such information means to measure, classify, and segment their target audiences while empirically testing the results of their indirect manipulations.

Casual mobile games exemplify an IUI that could deplete self-control, increase cognitive load, and present the user with the option to make decisions against their better judgment. Popular games – such as Clash of Clans, Candy Crush Saga, and Pokémon GO – feature numerous decisions that each seem vitally important yet don't generally alter the long-term course of a player's experience. Although game developers generally seek to increase revenue by improving the user's experience,[11] a deceitful actor could apply such techniques to exploit a user by presenting decisions precisely at times when the user is at a disadvantage.

Prospects for Mitigation

How can we mitigate the foregoing risks without losing the benefits of IUIs?

Ethical IUI Design

A straightforward approach is to push for stronger standards for ethics among content and service providers who create or utilize IUIs. A combination of industry standards, social norms, legislation, Institutional Review Board (IRB) practices, and certifications could mitigate some privacy concerns when deploying commercial services. Although some developers of IUIs consider complex ethical matters,[12] privacy doesn't have ubiquitous support due to numerous cultural factors that can make privacy appear to be a minor concern.[13]

Architectural Solutions and Open Standards

Sound architecture and algorithms can enhance privacy while allowing providers access to the data and analytics needed in IUIs. Differential privacy guarantees protection in some situations by adding noise or resampling data.[14] Contextual middleware[15] provides a high-level API to IUI apps that hides user-specific sensor data and reveals only the user's readiness for an intelligent action by the app. These two approaches could be adapted for IUIs by weakening the connection between the decisions needed in a game and the user's state.

User Agents

User agents – originating in a trusted operating system or device, and which reflect the user's interests – can help a user cope with privacy threats from IUIs. Similar techniques have proved valuable for low-level aspects, such as browser fingerprinting (for example, see Secret Agent; www.dephormation.org.uk/?page=81). Here we have in mind agents that accommodate richer models of threats to users than mere traceability of actions.

Agents could filter input data on the front end or notify a user when there's an increased risk of compromising sensitive information. For example, an agent could determine which data fields are necessary for a service and which are risky given the user's interests. An agent could provide correct data for legitimate purposes (the address needed for shipping) and fill in randomized data to enhance privacy in other cases (randomizing birthdates, for example, without affecting determination of adulthood).

Agents could filter on the back end, by monitoring content transmitted and API calls, such as Android and iOS support app permissions. Or the agent could act as a content-aware firewall and analyze and filter data before it's sent to the service provider. If a game is sending a user's contact list to a third party, such an agent could block the content from being sent.

Agents presuppose an open architecture. Given technological and legal ways – "walled gardens" – by which platform and content vendors restrict users' ability to automatically interact with software,[16] such agents might not be viable. This situation only highlights the need for openness, possibly through government regulation.

Economic Models

Defending yourself in an environment that includes hostile agents or contentious resources often requires nontrivial resource expenditure, or at least signaling a commitment to expend nontrivial resources, regardless of the domain. A person's private information and identity are valuable in many contexts, and IUIs are a key component in the arms race between privacy and exploitation, and between different vested interests, such as service providers and ad blockers.[17]

Game-theoretic approaches, which concern strategies of competing players (here, IUI providers and users), can help develop mechanisms that optimize some objective. We conjecture that techniques developed to protect physical infrastructure[18] can be enhanced for IUIs.

Provenance and Auditability

If we can store how analyses and actions are derived from some data, we can verify whether the data were used in a way unintended by the user. Blockchain technologies provide a way to store data (typically publicly) such that only holders of a cryptographic key can compute on and validate the content. Potentially, privacy-preserving blockchain contracts[19] might be extended to support a provenance mechanism, such that any transaction or analysis that depends on any other data could indicate which data it depends on without giving away the content.

As illustration, suppose an IUI provider is contractually bound to explain its decisions. That is, it might use personal data about users, but must store all analyses and decisions in a blockchain with references to specific data from which it was derived. A user could audit the blockchain to verify if any of his or her data was used for purposes outside the contract's scope. Tools would help perform the audit. This approach, however, is far from perfect. The relationships between the private data stored in the blockchain could reveal sensitive information about the user or trade secrets of the IUI provider.

People often find manipulation to be one of the most egregious personal violations – witness the controversy over Facebook's newsfeed manipulation.[20] Although manipulation might not involve information disclosure, it violates privacy by attacking a person's dignity. Because identity and integrity of autonomy are key to a person's sense of self, IUIs not only reveal a large attack surface but also expose particularly insidious risks. Understanding and addressing such risks is crucial for the future advancement of IUIs.

Improved methods are needed to help mitigate privacy risks, to balance privacy and utility. Methods involving architectures and agents are closest to practice; ideas from auditability and economics show promise as well.

Acknowledgment

Munindar Singh thanks the US Department of Defense for support through the Science of Security Lablet.

References

1. R. Liu et al., "An Unsupervised Collaborative Approach to Identifying Home and Work Locations," *Proc. 17th IEEE Int'l Conf. Mobile Data Management*, 2016; doi:10.1109/MDM.2016.53.
2. W.L. Prosser, "Privacy," *California Law Rev.*, vol. 48, no. 3, 1960, pp. 383–423.
3. Yahoo, "Belgian Woman Drives 3000km across Europe by Mistake," *Yahoo.com*, 16 Jan. 2013; https://nz.lifestyle.yahoo.com/travel/a/15850672/belgian-woman-drives-3000km-across-europe-by-mistake.
4. J. Nakamura and M. Csikszentmihalyi, "The Concept of Flow," *Handbook of Positive Psychology*, C.R. Snyder and S.J. Lopez, eds., Oxford Univ. Press, 2002, pp. 89–105.
5. T. Sala, "Game Design Theory Applied: The Flow Channel," *Gamasutra*, 8 Dec. 2013; www.gamasutra.com/blogs/ToniSala/20131208/206535/Game_Design_Theory_Applied_The_Flow_Channel.php.

6. P. Cortez and M.J. Embrechts, "Using Sensitivity Analysis and Visualization Techniques to Open Black Box Data Mining Models," *Information Sciences*, vol. 225, 2013, pp. 1–17.
7. C.W. Korn et al., "Depression Is Related to an Absence of Optimistically Biased Belief Updating about Future Life Events," *Psychological Medicine*, vol. 44, no. 03, 2014, pp. 579–592.
8. K.E. D'Anci, "Reduced-Calorie Diets and Mental Performance in Adults," *Nutrition and Mental Performance*, ch. 10, Macmillan, 2012, pp. 179–193.
9. M.S. Hagger and N.L.D. Chatzisarantis, "A Multi-Lab Pre-Registered Replication of the Ego-Depletion Effect," *Perspectives on Psychological Science*, vol. 11, no. 4, 2016, pp. 546–573.
10. C.R. Sunstein, *The Ethics of Nudging*, tech. report 2526341, Social Science Research Network, 2014; http://dx.doi.org/10.2139/ssrn.2526341.
11. J. Newman, J. Jerome, and C.J. Hazard, "Press Start to Track Privacy and the New Questions Posed by Modern Video Game Technology," *Am. Intellectual Property Law Association (AIPLA) Quarterly J.* vol. 42, no. 4, 2014, p. 527; www.aipla.org/learningcenter/library/books/qj/Pages/Quarterly-Journal-42-4.aspx.
12. V. Koenig, F. Boehm, and R. McCall, "Pervasive Gaming as a Potential Solution to Traffic Congestion: New Challenges Regarding Ethics, Privacy, and Trust," *Proc. Int'l Conf. Entertainment Computing*, LNCS 7522, Springer, 2012, pp. 586–593.
13. S. Cockcroft and S. Rekker, "The Relationship between Culture and Information Privacy Policy," *Electronic Markets*, vol. 26, no. 1, 2016, pp. 55–72.
14. C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, nos. 3–4, 2014, pp. 211–407.
15. P.K. Murukannaiah and M.P. Singh, "Platys: An Active Learning Framework for Place-Aware Application Development and Its Evaluation," *ACM Trans. Software Engineering and Methodology*, vol. 24, no. 3, 2015, pp. 19:1–19:32.
16. T. Sweeney, "Microsoft Wants to Monopolise Games Development on PC. We Must Fight It," *The Guardian*, 4 Mar. 2016; www.theguardian.com/technology/2016/mar/04/microsoft-monopolise-pc-games-development-epic-games-gears-of-war.
17. J. Constine, "Facebook Rolls out Code to Nullify Adblock Plus' Workaround Again," *Tech Crunch*, 11 Aug. 2016; https://techcrunch.com/2016/08/11/friendblock/.
18. M. Tambe, *Security and Game Theory*, Cambridge Univ. Press, 2011.
19. A. Kosba et al., "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Proc. IEEE Symp. Security and Privacy*, 2016, pp. 839–858.
20. G.S. McNeal, "Controversy Over Facebook Emotional Manipulation Study Grows as Timeline Becomes More Clear," *Forbes*, 30 June 2014; www.forbes.com/sites/gregorymcneal/2014/06/30/controversy-over-facebook-emotional-manipulation-study-grows-as-timeline-becomes-more-clear/#5de2f38a4e44.

Christopher J. Hazard is the founder of Hazardous Software (a game company known for the award-winning 2011 strategy game Achron). His work spans a variety of fields, including AI, trust and reputation, networks, cybersecurity, robotics, psychology, privacy, economics, and logistics. Hazard has a PhD in computer science from North Carolina State University. Contact him at cjhazard@hazardoussoftware.com.

Munindar P. Singh is a computer science professor at North Carolina State University. His research interests include the conception, engineering, and governance of sociotechnical systems as a way to tackle concerns such as security and privacy. Singh is an IEEE Fellow, a former Editor in Chief of *IEEE Internet Computing*, and the current Editor in Chief of *ACM Transactions on Internet Technology*. Contact him at singh@ncsu.edu.

This article originally appeared in IEEE Internet Computing, vol. 20, no. 6, 2016.