Author's version

There is more to Biometrics than User Identification: Making Mobile Interactions Personal, Secure and Representative

Daniel Buschek

Abstract: This essay contributes an extended view on user information inferred by personal devices to motivate applications of biometrics beyond user identification. We unfold a new design space in two parts: First, we take inspiration from the shared focus on individuality in both biometrics and Belk's Extended Self (ES, [1, 2]). ES describes that people use (digital) objects to define and reflect on their identities. Following this, we propose that personal devices can use biometrics to assess individual user attributes and behaviour for three application areas related to the core aspects of ES: privacy and security (Having), UI personalisation (Doing), digital self-presentation (Being). Second, we propose to view biometrics as part of a larger class of Implicit Information. Such information is inferred from interactions and sensors to be used across these application domains. We discuss implications and limitations of this view.

ACM CCS: Security and privacy → Human and societal aspects of security and privacy → Usability in security and privacy

Keywords: Biometrics; Mobile Device; Extended Self; Implicit Information

1 Introduction

Mobile devices such as smartphones serve as close companions in many everyday tasks. They thus collect rich data about their users, which needs to be protected to preserve privacy and security. Intriguingly, personal information can itself help to protect personal data. Jain and Ross defined such *biometrics* as "the science of establishing the identity of an individual based on physical, chemical, or behavioral attributes of the person" [19].

Indeed, many HCI researchers address privacy and security threats with biometric information, extracting user-specific features, for example, from fingerprints [17], voice [8], touch [6, 10, 24, 31] and typing behaviour [4, 31],

However, such user-specific information is also utilised in UI personalisation to tailor interfaces to an individual user (e.g. adapting touch keyboards [32]). It can also help to present the user to others, for example by personalising text messages [5, 18, 20, 29].

Such non-security use-cases are rarely associated with biometrics, although they require similar user-specific data and models. It may thus hinder progress if insights from, say, keyboard personalisation are not transferred to typing biometrics (as recently discussed [4]). Hence, HCI may benefit from a "holistic" cross-application perspective on 1) biometric information and 2) its possible applications. This essay contributes such a view:

1) We propose to view biometrics as part of a larger class of *Implicit Information*, which systems can infer from interactions and device sensors. This information-centric view facilitates exchange across use-cases: The same information may inform different applications.

2) We motivate use-cases for such information, in particular for biometrics, via *Extended Self* (ES) [1, 2], a concept from consumer research. Since ES and biometrics both focus on *individuality* of consumers/users of (digital) objects, the ability of biometrics to assess individual user attributes and behaviour can help applications to address user needs in areas related to three core ES functions: privacy and security (Having), UI personalisation (Doing), and self-presentation (Being).

In summary, ES motivates our interest in Having, Doing, and Being associated with user identity, while biometrics help to realise this association in interactive systems.

Discussing benefits and limitations of this view, we conclude with a case for holistic use of implicit (biometric) information, still to secure, but also to personalise and communicate an individual's characteristic interactions.

2 Design Space

Our user-centred (Extended Self) and system-centred view (Implicit Information) span a new design space (Table 1) that captures our extended perspective on biometrics for personal mobile devices. Crucially, it encompasses different applications of biometrics, also beyond security. This section develops the space in detail.

2.1 User View: Extended Self and Biometrics

Belk's concept of self extension describes that our possessions help us to define and reflect on our identities [1]. For example, we might value a travel souvenir as a reminder of a shaping experience and as a related conversation piece. More generally, Belk contrasts Sartre, Marx, and Fromm, to identify three functions of extended self: having, doing, and being. We refer to his work for details and further discussions [1, 2, 3].

2.1.1 Extended Self Inspires Biometric Applications

In this essay, we take three steps to connect self extension with biometrics on personal mobile devices:

First, we associate the three functions with mobile human-computer-interaction (HCI): Users own personal mobile devices (having), with which they interact (doing) and possibly define part of their self-view (being), for example being "modern and connected".

Second, we associate the functions with mobile user needs: Users want to avoid loss and theft of their devices and data (having – security needs). They want to master control over devices (doing – interaction needs), which in turn facilitates self extension [1], often to communicate effectively (being – presentation needs) [28]. Goals of doing and being have also been described as the very origins of user experience [14]. This supports our view to consider them as fundamental aspects in interactive systems, now also in those employing biometrics.

Third, we argue that biometric information can help to convincingly address these needs. For example, users want to avoid loss and theft of their devices and data (having). Biometrics offer protection based on how users act (doing) and who they are (being). This is the traditional security-centric view on biometrics; most applications of biometrics currently aim to identify or verify users in some way.

This essay aims to expand this security-centric view on biometrics by varying the focus on the three functions of self extension. We thus motivate three application areas, that each address one need, described in the following.

2.1.2 Biometrics and Having: Privacy/Security

In security applications, biometrics protect what we have (e.g. personal data) with what we do (e.g. typing behaviour [4]), and who we are (e.g. fingerprint [17]) – in addition to what we have (e.g. a connected authenticated smartwatch). Here, focus is on having (protection).

2.1.3 Biometrics and Doing: UI Personalisation

In interface personalisation (e.g. keyboard adaptation), biometrics enhance what we can do with the UI (e.g. typing fast and error-free), by enabling it to adapt to who we are (e.g. hand size), and how we interact (e.g. hand posture) – in addition to what we have (e.g. stylus or not). Here, focus is on doing (improved interaction).

2.1.4 Biometrics and Being: User Representation

In user representation (e.g. in a chat), biometrics help to communicate who we are by impacting on digital output that is shown to others (e.g. chat message), taking into account what we do (e.g. adapting font based on typing behaviour [5, 18]), and who we are (e.g. author name added based on fingerprints while typing [17]) – in addition to what we have (e.g. "sent from my iPhone"). Focus is on being (self-presentation of user to others).

2.2 System View: Implicit Information

To provide a comprehensive perspective, we consider biometrics as part of a more general class of *Implicit Information*, which systems can infer from interactions and device sensors. The purpose of this information-centric view is to highlight possibilities for exchange across use-cases: Once inferred for one application (e.g. security), systems may reuse the same information in other areas (e.g. UI personalisation). Our definitions loosely follow Schmidt's ideas on implicit interactions [25].

2.2.1 Definition of Implicit Information

We define Implicit Information in HCI as:

> Any information 1) inferred by an interactive computing system, 2) based on past and current observations of 3) users and how and in which context they perform interactions, 4) which by design do not solely serve the purpose of providing this information.

We comment on the definition's parts: 1) Implicit information is not explicitly provided to the system, it rather needs to be inferred from other data. 2) This data is measured by the system. 3) In particular, it measures biometric data, that describes user attributes and behaviour, but also context. 4) Implicit information is a "by-product" of an existing interaction that has a purpose for the user beyond generating data for inference.

Importantly, implicit information is a *superset* of biometric information. This essay's perspective and design space thus encompass not only inferred user identity but also other inferred factors, such as usage context, personality, tools, and so on (see examples in Table 1). We expect such information to be useful for the described applications, too, also in combination with biometrics.

2.2.2 Implicit Information Systems

An *Implicit Information System* is a computing system that infers, processes, and utilises implicit information. We can characterise such systems along five dimensions:

Focus	Dimension	Design Question	Examples
		Regarding the technical system	
System	Interactions	which interactions does it observe?	touching [6, 17, 30], typing [4, 5, 31, 32], unlocking [10, 24], speaking [8]
	Features	which features does it measure?	typing rhythm/speed [4, 5, 8], touch offsets [6, 30], fingerprints [17], finger trajectories [10, 24], grip pressure [16]
	Inference	how does it process its measurements?	regression [5, 30], classification [4, 8, 12, 24, 31, 13], anomaly detection [4], digital signal processing [8, 12, 16]
	Information	which information does it infer?	touch targeting characteristics [5, 6, 30], personality [7], identity [4, 6, 10, 17, 31], hand posture [12, 32], tools [13]
		How can the application	
User	Having	contribute to privacy and security?	user identification and verification when: typing [4, 8], unlocking [10], touching [6, 17], speaking [8]
	Doing	facilitate efficient & effective interaction?	keyboard personalisation [32], personal touch error compensation [30] and touch anticipation [22]
	Being	support digital self-presentation?	message personalisation [5, 18, 20, 29], call augmentation [16]

Table 1: Design Space for Implicit Information Systems regarding 1) technical methods and 2) application goals, motivated by ES.

They 1) observe different interactions 2) regarding different features, processed with 3) different methods to 4) derive different kinds of implicit information for 5) different applications (see Table 1).

3 Discussion and Implications

3.1 Implicitly Inferred (Biometric) Information

We discuss implications and benefits of our information-centric view on (biometric) systems in our design space.

Ubiquitous: Inferring implicit information can be considered a ubiquitous aspect of interest in HCI, since for *any* interaction we may measure typical (behavioural) biometrics and context.

"For free": To know about user and context, a system could ask the user explicitly (e.g. log-in prompt asks for identity). However, this usually comes with "costs" for the user, for example in terms of time and distraction. Hence, every bit of information that can be inferred implicitly (e.g. via biometrics) from the user's main task interactions (i.e. "for free" from the user's view) may save users' time and mitigate distraction.

Measurable: Many (biometric) inference systems are concerned with extracting certain "amounts" of implicit information. For example, consider that a device observes typing rhythm to distinguish its owner from attackers with, say, 80% accuracy. If it achieves 90% by observing touch offsets instead, we may conclude that there is measurably less identity information in typing rhythm than offsets. If formalised (e.g. [6]), the concept of Implicit Information can thus cast a quantitative perspective on interactions beyond usual measures like time and error rate: We can evaluate interactions in terms of which and how much implicit information they provide.

Facilitates exchange: Implicit Information facilitates exchange of methods and systems across applications. For example, recent work [4] has pointed out that spatial touch typing features well-known in keyboard personalisation had not yet been systematically explored for typing biometrics, although this area can greatly benefit from such individual features. We argue that Implicit Information in our design space highlights possibilities for exchange across use-cases via its information-centric view: The same interactions, features, methods, and inferred information may inform multiple applications.

3.2 Extended Biometric Application Areas

We reflect on the motivated application areas in detail.

3.2.1 Biometrics for UI Personalisation

Digital goods are rarely singular, since they can be duplicated endlessly and exactly. Belk [2] describes that digital possessions are thus less effective objects of self extension than physical ones, which might be hand-crafted or become "unique" to us through wear and tear.

Since UI personalisation provides users with ways of adapting and adopting digital goods (e.g. apps, messages), we argue that personalisation thus renders them more suitable for self extension: First, personalised UIs can increase effectiveness (e.g. [32]) and mastering control over objects facilitates self extension [1]. Second, related work [23] showed that UI personalisation and the following self-determination needs [9] are closely connected: 1) *Autonomy*, being the origin of personalisation that turns a default technology into the user's own. 2) *Competence*, when personalised UIs render the user's actions more effective. 3) *Relatedness*, when personalisation offers opportunities for expression of emotion and identity.

Hence, self extension and self-determination strongly motivate the use of biometrics in UI personalisation, since biometrics can capture important aspects of the user's self, such as unique behaviour and anatomy.

In particular, following keyboard adaptation research (e.g. [32]), we envision that other touch GUIs could also adapt to individual touch behaviour. For example, such touch characteristics could inform computational layout optimisation, aiming to place a user's most used GUI elements in the most accessible screen regions for that person and context (e.g. current hand posture).

Besides optimising GUIs for efficiency (i.e. addressing *Competence*), we suggest that revealing a user's individual ways of operating a GUI may prove interesting with regard to other needs (e.g. *Autonomy*, *Relatedness*). For example, GUIs could become more personal by showing "digital wear and tear", depending on how and where the user touches the most. Such visual traces of use could be beautifying, in contrast to traces of physical use (e.g. marking most touched areas in a subtle glow, inspired by heatmaps in website usage analysis). Personalising GUIs implicitly in this way could support "territory marking" [23], and would allow users to reflect on their past interactions, similar to ideas in personal informatics [21]. For example, traces of use in a contact list could highlight the most frequently called friends.

3.2.2 Biometrics for Self-Presentation

One benefit of self extension into objects is that they allow us to present ourselves and to encourage feedback from others who would be "reluctant to respond so openly to the unextended self" [1]. Such objects can be physical or digital (e.g. an avatar in a chat room) [2].

To reflect on this biometric application area, we thus now turn to use-cases where others can perceive our digital selves: computer-mediated communication (CMC). Following Walther's model of CMC [27], users utilise interface and channel properties to nudge the receiver's impressions towards a desired outcome. In CMC, users can better control self-presentation than in face-to-face communication [28], due to 1) editing messages, 2) generous drafting time, 3) cognitive focus on the message without need for environmental scanning, and 4) physical isolation from receivers, which hides non-verbal cues.

Thus, we argue that biometric systems can impact on self-presentation in (at least) two ways: First, since biometric information is user-specific, it can help users to present themselves as individuals. For example, rendering chat messages in the user's handwriting was perceived as more personal than normal fonts [5, 20]. Second, biometrics can re-introduce non-verbal cues into CMC. For example, adapting fonts based on movement and typing behaviour enables receivers to infer if the message was written while walking [5]. In another example, grip pressure during a phone call served as a non-verbal channel by triggering vibration on the receiver's end [16].

These impacts can be desirable (e.g. a font showing walking might excuse briefness) or not (e.g. walking might be understood as not focusing on the conversation). This essay views self-presentation as a strong motivation and relevant area for future HCI research on biometrics, since employing biometric information for self-presentation may be as useful as it is challenging to "get right" for users in practice. More options to influence messages for self-presentation might increase both reviewing/editing and message immediacy [28]. Hence, such applications must in particular offer a suitable degree of control over biometric information shared with others (see e.g. [15]).

3.2.3 Biometrics for Usable Privacy and Security

Finally, we return to the traditional application of biometrics. Here we note that the user-centred dimensions of our design space highlight that biometric systems can at once (i.e. using the same data and methods) address privacy/security and other applications. For example, handwriting is a useful biometric to identify users [26]. This security application could be combined with:

1) UI personalisation: Recent work [11] has investigated how personalising the UI by rendering text in the user's own handwriting can mitigate shoulder surfing risks.

2) Self-Presentation: Receivers of text messages rendered in a personalised handwritten font can to some extent distinguish typists [5]. This could serve as an additional cue for receivers to determine if a message was really sent by the person it claims to be coming from.

More generally, we hope that this essay's perspective and design space facilitate and inspire further exploration of such cross-application uses of biometric systems, including, but going beyond, privacy and security.

3.3 Critique and Limitations

Here we address critical questions on the proposed view.

Which limitations come with the ES motivation? There may certainly be 1) further application areas for data on individual user characteristics, as well as 2) concepts *within* each of the areas motivated in this essay, which cannot be motivated by ES. For example, within the privacy/security area, ES cannot account for knowledge-based authentication, since Belk's "having" originally only refers to physical property, not possession of knowledge [1]. Although Belk later revisited ES to include digital possessions as well [2], it may be far-fetched to include, say, passwords here. However, passwords are neither biometrics nor implicit information and thus not in the proposed design space. Finally, ES itself is only one of several similar concepts [3], each of which may introduce its own narrowing focus.

Is the design space putting "old wine in a new bottle"? The design space aims to highlight connections between existing research areas in HCI, including topics from usable privacy/security, UI personalisation, CMC. Considering their shared interest in user-specific information, we hope to inspire *new crossovers*, which then lead to novel applications. In particular, we motivate holistic biometric systems, which use the same user (behaviour) data to verify identity, and personalise UI and output.

Can biometric systems "know too much"? This is no new concern, but it should be taken all the more seriously for cross-application use of biometrics: In particular, using biometrics for self-presentation reveals additional information about the user. This may contradict parallel applications that employ biometrics to protect the user's privacy. This hints at tradeoffs between application goals, raising important questions for usable privacy and security research. As a general guideline, we argue that systems should 1) clearly communicate to the user which information is inferred and utilised for which application, and 2) provide control over such processes.

Is this a culturally limited perspective? Extended Self is a highly individualistic concept. It may thus not apply or appeal equally well to all cultures and at all times [1]. This may negatively affect its suitability to motivate some application areas for some user groups. However, such limitations are not suddenly introduced by this essay – interest in biometrics is inherently tied to interest in individuality of humans and human behaviour.

4 Conclusion

This essay has proposed a novel perspective on biometrics as a subset of *Implicit Information* which can be inferred by personal mobile devices from interactions and sensors. The purpose of this view is to highlight connections between different application areas of such information, including areas previously rarely associated with biometrics. We motivated three particular application areas via Belk's *Extended Self* as user-centred dimensions in a novel design space. We discussed how this design space motivates "holistic" biometric systems that use inferred information across multiple areas.

Regarding the broader topic, we thus conclude that "usable privacy and security" might not have to end with addressing usability of security applications. It could rather also include (re-)using user information, originally motivated and extracted by privacy/security systems, to address other user needs. In particular, this essay motivated applications for efficient and effective interactions with personalised UIs, and novel opportunities for users to digitally present themselves to others.

Literature

[1] Belk, R. W. *Possessions and the Extended Self.* Journal of Consumer Research, 15(2), 139-168, 1988.

[2] Belk, R. W. *Extended Self in a Digital World.* Journal of Consumer Research, 40(3), 477-500, 2013.

[3] Belk, R. *Alternative Conceptualizations of the Extended Self.* Advances in Consumer Research, 42, pp. 251-254, 2014.

[4] Buschek, D., De Luca, A., and Alt, F. *Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1393-1402, Seoul, South Korea, April 18 - 23, 2015.

[5] Buschek, D., De Luca, A., and Alt, F. *There is more to Typing than Speed: Expressive Mobile Touch Keyboards via Dynamic Font Personalisation.* Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 125-130, Copenhagen, Denmark, August 24-27, 2015.

[6] Buschek, D., De Luca, A., and Alt, F. *Evaluating the Influence of Targets and Hand Postures on Touch-based Behavioural Biometrics.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, May 7-12, 2016.

[7] Chittaranjan, G., Jan, B., and Gatica-Perez, D. *Who's who with big-five: Analyzing and classifying personality traits with smartphones.* International Symposium on Wearable Computers, pp. 29-36, June 12-15, 2011.

[8] Crawford, H., Renaud, K., and Storer, T. *A framework for continuous, transparent mobile device authentication.* Computers & Security, 39, pp. 127-136, 2013.

[9] Deci, E.L., Ryan, R.M. *The "what" and "why" of goal pursuits: Human needs and the self-determination of behaviour.* Psychological Inquiry 11, 227-268, 2000.

[10] De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. *Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 987-996, Austin, Texas, USA, May 5-10, 2012.

[11] Eiband, M., Von Zezschwitz, E., and Buschek, D. *My Scrawl Hides It All: Protecting Text Messages Against Shoulder Surfing With Handwritten Fonts.* CHI '16 Extended Abstracts, San Jose, CA, USA, May 7-12, 2016.

[12] Goel, M., Wobbrock, J. O., and Patel, S. N. *GripSense: Using Built-In Sensors to Detect Hand Posture and Pressure on Commodity Mobile Phones.* Proceedings of the ACM Symposium on User Interface Software and Technology, pp. 545-554, Cambridge, Massachusetts, USA, October 7-10, 2012.

[13] Harrison, C., Schwarz, J., and Hudson, S. *TapSense: Enhancing Finger Interaction on Touch Surfaces.* Proceedings of the ACM Symposium on User Interface Software and Technology, pp. 627-634, Santa Barbara, CA, USA, October 16-19, 2011.

[14] Hassenzahl, M. *User experience (UX): Towards an experiential perspective on product quality.* Proceedings of the 20th Conference on L'Interaction Homme-Machine, pp. 11-15, 2008.

[15] Hassib, M., Khamis, M., Schneegass, S., Shirazi, A. S., and Alt, F. *Investigating User Needs for Bio-sensing and Affective Wearables.* Extended Abstracts of the 34th SIGCHI Conference on Human Factors in Computing Systems. San Jose, CA, USA, May 7 - 12, 2016.

[16] Hoggan, E., Stewart, C., and Haverinen, L. *Pressages: Augmenting Phone Calls with Non-Verbal Messages.* Proceedings of the ACM Symposium on User Interface Software and Technology, pp. 555-562, Cambridge, Massachusetts, USA, October 7-10, 2012.

[17] Holz, C., and Baudisch, P. *Fiberio: A Touchscreen that Senses Fingerprints.* Proceedings of the ACM Symposium on User Interface Software and Technology, pp. 41-50, St. Andrews, Scotland, United Kingdom, October 8-11, 2013.

[18] Iwasaki, K., Miyaki, T., and Rekimoto, J. *Expressive Typing: A New Way to Sense Typing Pressure and Its Applications.* In CHI '09 Extended Abstracts, pp. 4369-4374, Boston, MA, USA, April 4-9, 2009.

[19] Jain, A., Flynn P., and Ross, Arun A. (Eds.). *Handbook of Biometrics.* Springer Science & Business Media, 2007.

[20] Kienzle, W., and Hinckley, K. *Writing Handwritten Messages on a Small Touchscreen.* Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 179-182, Munich, Germany, August 27-30, 2013.

[21] Li, I., Dey, A., and Forlizzi, J. *A Stage-Based Model of Personal Informatics Systems.* Proceedings of the SIG-

CHI Conference on Human Factors in Computing Systems, pp. 557-566, Atlanta, Georgia, USA, April 10-15, 2010.

[22] Mohd Noor, M. F., Ramsay, A., Hughes, S., Rogers, S., Williamson, J., and Murray-Smith, R. *28 Frames Later: Predicting Screen Touches from Back-of-device Grip Changes.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2005-2008, Toronto, Ontario, Canada. 2013.

[23] Oulasvirta, A., and Blom, J. *Motivations in personalisation behaviour.* Interacting with Computers, 20(1), 1-16, 2008.

[24] Sae-Bae, N., Ahmed, K., Isbister, K., and Memon, N. *Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 977-986, Austin, Texas, USA, May 5-10, 2012.

[25] Schmidt, A. *Implicit Human Computer Interaction Through Context.* Personal Technologies, 4(2-3),191-199. 2000.

[26] Srihari, S. N., Cha, S.-H., Arora, H., and Lee, S. *Individuality of Handwriting.* Journal of Forensic Sciences, 47(4), 1-17. 2002

[27] Walther, J. B.*Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction.* Communication Research, 23(1), 3-43, 1996.

[28] Walther, J. B. *Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language, and cognition.* Computers in Human Behavior, 23(5), 2538-2557, 2007.

[29] Wang, H., Prendinger, H., and Igarashi, T. *Communicating Emotions in Online Chat Using Physiological Sensors and Animated Text.* In CHI '04 Extended Abstracts, pp. 1171-1174, Vienna, Austria, April 24-29, 2004.

[30] Weir, D., Rogers, S., Murray-Smith, R., and Löchtefeld, M. *A User-Specific Machine Learning Approach for Improving Touch Accuracy on Mobile Devices.* Proceedings of the ACM Symposium on User Interface Software and Technology, pp. 465-476, Cambridge, Massachusetts, USA, October 7-10, 2012.

[31] Xu, H., Zhou, Y., and Lyu, M. *Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones.* Symposium On Usable Privacy and Security, pp. 187-198, Ottawa, Canada, July 22-24, 2014.

[32] Yin, Y., Ouyang, T. Y., Partridge, K., and Zhai, S. *Making Touchscreen Keyboards Adaptive to Keys, Hand Postures, and Individuals - A Hierarchical Spatial Backoff Model Approach.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2775-2784, Paris, France, April 27 - May 2, 2013.

M.Sc. Daniel Buschek graduated with a Master's degree in Media Informatics from the University of Munich in 2013. His studies focused on machine learning for mobile touch devices, including an internship at the University of Glasgow, and work as a research assistant at the Helsinki Institute for Information Technology. Since 2014, he is a Doctoral researcher in the Media Informatics group at the University of Munich, with particular interest in user-specific behavior evident in interactions with mobile touch devices.

Address: Ludwig-Maximilians-Universität München (LMU), Media Informatics Group, Amalienstrasse 17, 80333 München
E-Mail: daniel.buschek@ifi.lmu.de