Digital Behavioral Biometrics and Privacy: Methods for Improving Business Processes without Compromising Customer Privacy

J.S. Valacich*, J.L. Jenkins** and D. Čišić***
* University of Arizona/Management Information Systems Department, Tucson, AZ, USA
** Brigham Young University/Information Systems Department, Provo, UT, USA
*** University of Rijeka/Department of Informatics, Rijeka, Croatia
valacich@arizona.edu

***Abstract* - To enable people to interact with online websites and systems, browsers capture a variety of events that occur on the page—such as how a person is moving the computer mouse, what a person clicks on, what a person types, and whether a person is scrolling. These events represent a user's behavior on a page, referred to as the DOM or Document Object Model, and are recorded at a millisecond precision rate (e.g., the exact millisecond timestamp when a key goes down and when it comes back up). Research and practice alike have found that these behavioral events can provide powerful insight into the users' experience, such as whether users are frustrated, and even help distinguish between legitimate and fraudulent users. In this paper, we present six best practices for responsibly collecting these digital behavioral biometric data to help protect user privacy as well as encourage proper interpretation. For each principle, we discuss its rationale and practical application.**

Keywords – digital behavioral biometric, security, privacy, document object model (DOM) events

I. Introduction

There is a large and growing literature focusing on understanding user behavior when interacting with websites [1]. For instance, most commercial websites capture a variety of information including device information (e.g., geolocation, operating system and browser versions, screen resolutions, etc.) as well as various types of user behavior information such as the amount of time spent on a particular page as well as measures of various actions the user had taken such as rating a product, clicking a link, or booking an airline flight. In addition to these specific behavioral activities, there is also a rapidly growing and evolving field that analyses how the user typed an entry or used their mouse to navigate and make choices. This emerging field falls under a concept called behavioral biometrics [2], which focuses on the measurement of various human *behaviors* such as how a person walks or talks. Such behaviors can be unique to an individual and can be used to segment a population into different groups based on their behavior.

Prior research has established that individuals have repeatable and predictable behavioral biometrics [2]. These behavioral signatures are not limited to how a person walks or talks but also includes how a person interacts with a computer or smartphone. In a computer security context, *digital behavioral biometrics* (DBB) has primarily been used in authentication contexts [2], but is increasingly being used to understand users' cognitive and emotional states such as the level of user deception, cognitive load, and frustration [e.g., 3].

In this paper, we briefly provide some background on the Document Object Model (DOM), and how the DOM enables the collection of a rich set of events when a person interacts with a webpage—the foundation for digital behavioral biometrics. In this description we explain how DOM events are collected, describe prior research that has used such events to infer cognitive and emotional changes in users, and how metrics related to behavior can be constructed. We then describe how these metrics can be used to improve various online business processes. Finally, we describe six best practices for improving user privacy and security when collecting and analyzing DOM events.

II. Background

Before introducing best practices for collecting and interpreting digital behavioral biometric data, we first introduce the practice of collecting DOM events, the science of interpreting such events, and details on how to translate DOM events into digital behavioral biometric measures.

A. DOM Event Collection

The Document Object Model (DOM) refers to a webpage that is loaded in a browser. It contains a tree of all elements, attributes, and related data on an HTML page (e.g., buttons, textboxes, images, styles, etc.) (https://www.w3schools.com/js/js_htmldom.asp). When users interact with the DOM, events are triggered. For example, when a person clicks on a button, a "click" event is triggered. This allows the browser to detect behaviors and execute appropriate actions (e.g., when an "add to cart" button is clicked, a product is added to the shopping cart). The list of DOM events that can be triggered is extensive but is well documented (e.g., https://www.w3schools.com/jsref/dom_obj_event.asp, https://developer.mozilla.org/en-US/docs/Web/API). For illustration, Table I provides a sample of events that can be triggered in the DOM.

JavaScript—a programming language that can be run within a browser—can "listen" for events. An Event Listener is a technical term that refers to a procedure that waits for an event to be triggered. When an event is triggered, the event listener will execute code, referred to as a handler. For example, a handler for a "add to cart" button will include the code to add a product to a shopping cart in an ecommerce website. In the context of DBB, the handler may simply record the event, or send it to a server, for further analysis. Event listeners can be configured using basic JavaScript or through third party libraries, such as jQuery (https://jquery.com/). Table II provides example code of adding event listeners.

TABLE I. ILLUSTRATIVE EXAMPLES OF EVENTS THAT CAN BE TRIGGERED IN THE DOM

Event	*Triggered when a user…*
click	clicks on an element
focus	gives focus (e.g., clicks in) to an element
blur	loses focus (e.g., clicks out of) an element
keydown	presses a key down
keyup	releases a key
mousemove	moves the mouse cursor
scroll	scrolls on a scrollbar
touchstart	places a finger on a touchscreen
touchend	removes a finger from a touchscreen
input	enters information into an element

TABLE II. EXAMPLES OF ADDING EVENT LISTENERS

Method	*Code*
Plain JavaScript	document.getElementById("myBtn").addEventListener("click", function() { /*write code to perform an action here */ });
jQuery	$("#addToCartButton").click(function() {/* write code to perform an action here*/ });

B. Science of Using DOM Events to Understand Users

JavaScript can listen for DOM events and save them or send them to a server for analysis. Research has shown that the analysis of such events can provide insight into users emotional and cognitive states. Over the past decade, scholars in cognitive and neurological sciences have unequivocally demonstrated that fine motor control is influenced by cognitive and emotional changes [4]. As such, the tracking of mouse movements as well as interaction data from touch screens, keyboards, and various other input devices – i.e., digital behavioral biometrics – has become a scientific methodology [2], broadly referred to here as *human-computer interaction (HCI) dynamics*, that is used to provide objective data about a person's decision making and other psychological processes. In a concise review of HCI dynamics, focusing on mouse tracking studies, Freeman, Dale and Farmer [4] suggest that the

"movements of the hand…offer continuous streams of output that can reveal ongoing dynamics of [cognitive] processing, potentially capturing the mind in motion with fine-grained temporal sensitivity."

Accordingly, numerous recent studies have chosen HCI dynamics as a methodology for studying various cognitive and emotional processes. For example, HCI dynamics have been shown to predict decision conflict [5], attitude formation, concealment of racial prejudices [6], response difficulty [7], response certainty [8], dynamic cognitive competition changes [9], perception formation [10], and emotional reactions [3], to name a few.

C. Translating DOM Events into Digital Behavioral Biometrics to Understand User Behavior

In the realm of DBB, there is a large and growing literature evaluating how users enter information and interact with various computing devices. For instance, *keystroke dynamics* (a type of HCI dynamics) refers to the detailed timing information that describes exactly when each key is pressed and when it is released while a person is typing on a computer-based keyboard or smartphone. Past research shows that individuals have repeatable and predictable keystroke dynamics [11].

To capture and calculate keystroke dynamics, you capture the time when a key is pressed and when it is released (Figure 1). With this data, two common metrics are calculated: 1) Dwell time: the time duration that a key is pressed, and 2) Flight time: the time duration in between releasing a key and pressing the next key.

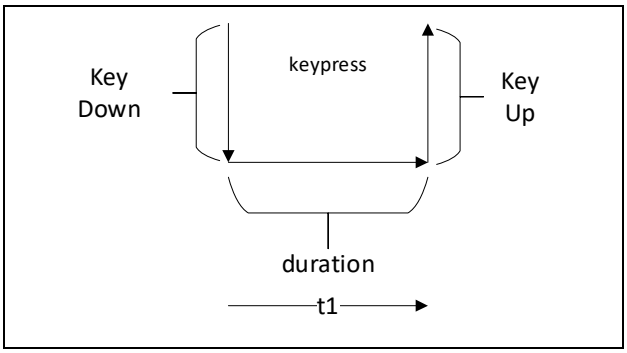

Figure 1. A keypress begins with a key-down event, a duration, and a key-up event.

Because modern keyboards allow a person to hold more than one letter, number, or symbol key down at the same time while transitioning from one key to the next (i.e., called an *over*-press), flight time can be a positive or negative number. From this data, different types of metrics can be generated (see Table III) [11].

TABLE III. EXAMPLES OF KEYSTROKE DYNAMICS METRICS

Keypress Duration Metrics	*Flight Time Metrics*
• Mean duration per field • Variance per field • Fastest keypress • Slowest keypress	• Mean flight time per field • Transition breaks (e.g., > 2 SD) • Over-press (binary) • Over-press ratio to total transitions

In a similar way, how a person utilizes a computer mouse – speed, accuracy, click timing, etc. – has repeatable and predictable patterns. These patterns can be calculated

using a variety of metrics and are referred to as mouse cursor dynamics [12]. For instance, in Figure 2, as a person moves the mouse from point A to B, metrics can be calculated by examining both movement behavior and time. For instance, by dividing the actual trajectory distance by the duration of movement, an average movement speed can be calculated [3]. In addition to keyboards and mice, other HCI devices and methods can be used to generate a rich set of metrics.

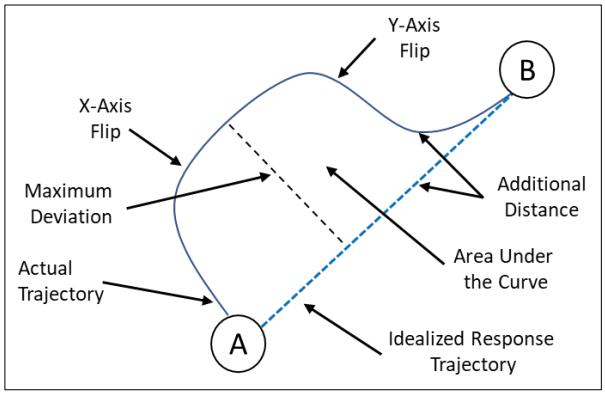

Figure 2. Examples of metrics from mouse movements.

III. Use Cases For HCI Dynamics

There is increasing use of customer interaction behavioral data to understand different types of users [13]. For instance, ecommerce sellers are using tools like Google Analytics (https://analytics.google.com/) to learn more about customers (e.g., device type, browser used, where they come from, default language, etc.) and their behavior on a website (e.g., what pages were visited, duration per page, images or links clicked, etc.) [14]. With behavioral biometric data, organizations can gain a deeper understanding of the cognitive and emotional states of that user, and ultimately develop unique personas based on behavioral commonalities [15]. For instance, examples of e-commerce personas include product-focused, browsers, researchers, bargain hunters, and one-time shoppers [16].

Increasingly, organizations are utilizing HCI dynamics to create a more granular and deeper understanding of users that visit their websites. For example, mousing dynamics can be used to predict if a user is feeling frustration on a website [3], experiencing low usability [17], feeling negative affect [18], or experiencing high cognitive load [19]. Beyond typical A-B testing, these insights can be used to *pinpoint* the exact location of customer experience problems, thus guiding where website usability improvements should be made, ultimately resulting in higher conversion and happier customers [15]. Beyond these examples, by linking online behaviors (assuming a high volume of customers) with important business outcomes (e.g., did a customer make a purchase?), custom predictive models can be generated to predict in real-time how the user is likely to behave in the future, allowing a website to dynamically adjust to accommodate the needs of the user [13].

Furthermore, DBB can be used to identify low quality and even fraudulent data entered into online forms and applications. Research has shown that mouse cursor and typing dynamics can be a powerful indicator of fraud when users are submitting insurance claims [20], entering information in text fields [21], and responding to investigatory surveys [12]. Likewise, mousing dynamics can be used to understand biases in survey responses [22]. On a security front, mouse cursor dynamics have been shown to be an effective data source to determine optimal times to display security warnings to improve adherence [23], and typing dynamics have been shown to be an effective method for predicting and decreasing password reuse [24]. Indeed, the collection and analysis of behavioral biometric data, as captured through DOM events, provides powerful insight into end user behavior.

IV. Best Practices to Protect User Privacy

As the use of digital behavioral biometrics can provide powerful insights into users' cognitive and emotional states, researchers and practitioners alike have a responsibility to protect users' privacy and security during the collection, analysis, and interpretation of DOM events. Below we highlight six best practices for protecting user privacy while analyzing DBB data.

A. Remove personally identifiable information from behavioral data when possible.

As more people utilize various computer technologies to communicate and engage in a broad range of online activities, the protection and privacy of their personally identifiable information (PII) has become a paramount concern. PII refers to any information related to an identified or identifiable natural person (see https://www.gdpr.org for more information). Such information includes various details such as your name, identification number, and location, but also combinations of factors that are specific to the individual that could be merged to possibly identify an individual. Examples include various physical and physiological factors, including DBB.

When collecting DBB data, care should be taken to avoid collecting PII in DOM events. Some events, by default, can contain PII that is not central to realize the benefits of DBB. For example, to continually authenticate a user using keystroke dynamics, it does not require knowing what was typed; rather, it only requires information about transition and duration characteristics of how keys were pressed, which only requires keypress timing data [25]. Hence, when collecting DOM events, the events should be sanitized (e.g., PII should be removed). Table IV provides examples of PII that should be removed from events prior to collecting them for analysis.

TABLE IV. Examples of Removing PII From Events

Event	***Example Event Sanitization***
keydown	Remove information regarding what alpha-numeric key was pressed (e.g., the alpha-numeric key code and alpha-numeric key value)
input	Remove the data with the inserted characters
change	Remove information about what the element was specifically changed to

B. Avoid intrusive events that require special permission.

Some digital behavioral-biometric data is intrusive and requires special permissions. Such data should be avoided, when possible. For example, through JavaScript, you can technically request permissions to access the computer camera and microphone. However, requesting camera and microphone data pierces a privacy boundary—namely, it reaches beyond the realm of the website and into the realm of the user. Aside from sound and video being PII, collecting it irresponsibly violates consumer protection laws. For example, in addition to requiring two-way consent to collect video and audio feeds under many jurisdictions, GDPR (General Data Protection Regulation) also requires that the purpose of the recording or processing fulfills one of a limited set of conditions outlined in Article 6 of GDPR (https://gdpr-info.eu/art-6-gdpr/):

> *"1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
>
> *2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
>
> *3. processing is necessary for compliance with a legal obligation to which the controller is subject;*
>
> *4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
>
> *5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
>
> *6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

C. Scope events within relevant domains.

As discussed in the previous best practice, the HCI world can be divided up into two realms: the user realm and the web realm. The *user realm* refers to the physical world the user lives in—e.g., a computer at a desk with a person sitting in front of it, inside of a house on a street in a neighborhood. The *web realm* refers to the information (e.g., websites and resources) that people can access via the computer. HCI devices—the computer mouse, keyboard, microphone, etc.—act as the interface between the user realm and the web realm. As previously mentioned, digital behavioral biometric events captured through HCI events that pierce unnecessarily into the user realm (e.g., cameras, microphones) should be avoided when possible.

In addition, the web realm can be split into multiple domains (see Figure 3)—these often equate to literal web domains or areas of ownership. For example, a website such as Amazon is on a different domain than HSBC bank. DBB collection should normally be limited to the domain that approves the collection. This can be accomplished by installing a behavioral biometric script on the domain's web resources. However, tools that allow digital behavioral biometric tracking across domains, such as browser plugins, should be avoided, especially when the tracking is extended to domains that have not approved said tracking.

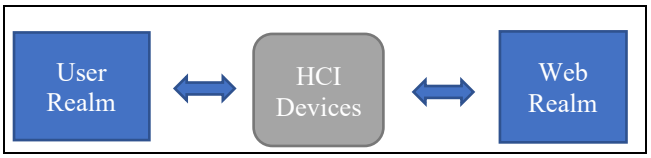

Figure 3. Each web domain should have independent polies regarding digital behavioral biometric data.

D. Encrypt behavioral biometric data during transit.

As HCI Devices act as the interface between the user realm and the web realm, they transfer information back to the appropriate domains. Although PII may have been removed from the events, they should still be protected as if they still contained sensitive information. A major element of protection involves encrypting data as it is transferred from HCI devices to the appropriate domains. Such protection is enabled by using strong transport protocols to prevent unsanctioned individuals from eavesdropping on customer data while it moves over the internet.

Ideally, this should be done using a modern Transport Layer Security (TLS) protocol to encrypt the data during transmission. In addition, data can be obfuscated by the JavaScript prior to transport to help further protect the data. Obfuscation techniques can include using codes to represent events, limiting what event information is sent up, and encoding the data.

E. Interpret events within context.

To make a valid inference of a person's cognitive and emotional states using DBB, one must account for the context. There are at least two major contextual factors that must be considered when analyzing and interpreting events: individual characteristics and the DOM target.

First, one must account for individual contextual factors when interpreting behavioral events. *Individual contextual factors* refer to the characteristics of the user that may make interpreting differences between users difficult. For example, users type at different speeds, possess different fine motor control abilities, have touch pads with different sensitivity, and even have screens with different resolutions. When making inferences based on DOM events, it is therefore important to account for "what is normal" for a given user, and then base interpretations of emotional and cognitive states based on deviations from that norm. For example, research shows that decreased mouse-movement speed is an indicator of increased cognitive load [19]. However, this interpretation can be biased for users who naturally move the mouse slower or faster than others despite cognitive load levels. Accounting for this individual difference allows a more accurate interpretation of the events.

Likewise, one must account for the target on the page that a user is interacting with. For example, one cognitive state that can be inferred from keystroke dynamics is familiarity with information [24]. Familiarity, in turn, is

used as an indicator of several outcomes such as information mastery [8] or even fraud [20]. For example, low familiarity when entering your name is often an indicator of fraud; normally, people have high familiarity when entering their name because they have typed it many times before. However, if you take a different target other than name, low familiarity may not be an indicator of fraud. For instance, some applications ask for your work address. Many have not memorized their work address, nor have much practice entering it. Hence, they would type work address with low familiarity. However, this is likely not an indicator of fraud. See Table V for examples of various contextual factors influencing digital behavioral biometrics.

TABLE V. EXAMPLES OF INDIVIDUAL CONTEXTUAL FACTORS

Event	***Example Event Sanitization***
Typing efficacy	People naturally type at different speeds.
Mousing speed	People may naturally move at different speeds, and mousing devices (touchpad, mouse) very often have different sensitivities.
Familiarity with website	People may have different prior experiences with the website which will influence how they interact with a webpage.
Screen resolution	Screens have different resolutions which will impact how many pixels (which is a unitless measure) that people move when navigating a webpage.

These examples show that DBB must be interpreted within the context of the target being interacted with. A certain DBB statistic (such as familiarity) may mean a very different thing on one target (e.g., first name) compared to another target (e.g., work address).

F. Base interpretations on science.

Interpreting DBB to make inferences about users should be founded in science. For example, the validity of using HCI dynamics for inferring changes in cognitive and emotional states is based on several foundational theories. Together, these theories explain how cognitive and emotional changes influence fine motor control, and thereby user's interactions with HCI devices. When a person moves a computer mouse, these movements can be described using three general variables: speed, distance, and direction. If a person could move a mouse perfectly from point-to-point, they would be able to maximize all three of these variables, resulting in movements that are fast and precise even over large distances. Such perfect execution is referred to as the *idealized response trajectory* (IRT)—a vector between two points [26]. Operationally, however, humans have limited capacity for making fine motor control movements, resulting in tradeoffs between these variables [27].

To compensate for these tradeoffs, motor movements are generally not executed in a single step that perfectly matches the IRT, but rather as a series of increasingly precise submovements that ultimately reach the target. This is more thoroughly described in the *stochastic optimized submovement model* [28]. This theory describes movements as consisting of a large, relatively fast, and imprecise initial movement toward a target followed by a series of smaller, slower, and more precise corrective submovements until the target is reached (Figure 4). Any deviations from the IRT will increase the distance of the movement, requiring a trajectory change to realign with the target. Submovements are increasingly slower and more precise as the target location is reached. These deviations from the IRT are used to measure spatial (i.e., distance and number of direction changes) and temporal (i.e., speed and duration) features that are indicative of the level of cognitive competition present in the movement [29].

In addition, when multiple potential targets are present, each potentially actionable target further influences the movement. This concept is described by the *Response Activation Model (RAM)* [30]. According to the RAM, when a person wants to move the hand to a stimulus (whether it be moving a mouse, typing on a keyboard, or touching the screen), the brain starts to prime a movement response toward the stimulus by transmitting nerve impulses to the hand and arm muscles toward the possible responses. However, the resulting movement is not only influenced by this intended movement, it is influenced by all stimuli with action-based potential [31]. A stimulus with *action-based potential* refers to any, potentially multiple, stimuli that *could* capture a person's attention [30]. For example, consider the context of a consumer rating a product they have purchased on an ecommerce website, stimuli with actionable potential may include all answers that capture a person's attention (e.g., "Should I choose the 4-star or 5-star response?"). When two or more stimuli, even briefly, capture a person's attention, responses to both stimuli are programmed in parallel [30]. This is an automatic, subconscious process that allows the body to react more quickly to stimuli that a person may eventually decide to move towards. The process of changing human fine motor control as cognitive competition occurs can be conceptualized and measured using any HCI device.

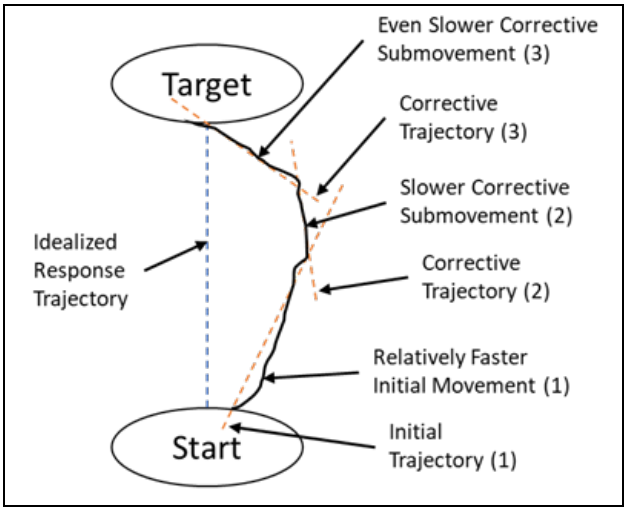

Figure 4. Mouse-cursor movements as described by the stochastic optimized submovement model

In addition to utilizing theory to inform accurate measurement and understanding, it is critical that strong controls be used when capturing and analyzing HCI dynamics to eliminate bias and aid in deriving accurate interpretation. For instance, in a scenario where A-B testing is evaluating website usability, it is critical that the

assignment of users to system A or B be randomly assigned, as well as include all types of users relevant to the context (e.g., to eliminate a coverage bias). Insights derived from strong theory and rigorous research design, will lead to a deeper and less-biased understanding of the meaning of DBB data.

V. CONCLUSION

We described the Document Object Model (DOM) and how it enables the collection of a rich set of events when a person interacts with a webpage. We also described how DOM events are collected, how they can be used to infer cognitive and emotional changes in users, and how these digital behavioral biometrics, can be constructed using concepts related to HCI dynamics. We then described how these metrics can be used to inform a broad range of online contexts. We conclude by reviewing six best practices for responsibly collecting this digital behavioral biometric data to help protect user privacy as well as encourage proper interpretation.

REFERENCES

[1] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E.P. Markatos. User tracking in the post-cookie era: How websites bypass GDPR consent to track users. in Web Conference. 2021. Virtual.

[2] K. Saeed, New directions in behavioral biometrics. 2016, Boca Raton, FL: CRC Press.

[3] M.T. Hibbeln, J.L. Jenkins, C. Schneider, J. Valacich, and M. Weinmann, "How is your user feeling? Inferring emotion through human-computer interaction devices," MIS Quarterly, 2017. vol. 41(1): p. 1-21.

[4] J. Freeman, R. Dale, and T. Farmer, "Hand in motion reveals mind in motion," Frontiers in Psychology, 2011. vol. 2: p. 59.

[5] C. McKinstry, R. Dale, and M.J. Spivey, "Action dynamics reveal parallel competition in decision making," Psychological Science, 2008. vol. 19(1): p. 22-24.

[6] M.T. Wojnowicz, M.J. Ferguson, R. Dale, and M.J. Spivey, "The self-organization of explicit attitudes," Psychological Science, 2009. vol. 20(11): p. 1428-1435.

[7] R. Horwitz, F. Kreuter, and F. Conrad, "Using mouse movements to predict web survey response difficulty," Social Science Computer Review, 2017. vol. 35(3): p. 388-405.

[8] J.L. Jenkins, et al. A multi-experimental examination of analyzing mouse cursor trajectories to gauge subject uncertainty. in Americas Conference on Information Systems. 2015. Fajardo, Puerto Rico.

[9] R. Dale, C. Kehoe, and M.J. Spivey, "Graded motor responses in the time course of categorizing atypical exemplars," Memory & Cognition, 2007. vol. 35(1): p. 15-28.

[10] J. Cloutier, J.B. Freeman, and N. Ambady, "Investigating the early stages of person perception: The asymmetry of social categorization by sex vs. age," PloS One, 2014. vol. 9(1).

[11] J.S. Valacich and J.L. Jenkins, Fraudulent application detection system and method of use. 2019, U.S. Patent No.10,248,804.

[12] J.L. Jenkins, J. Proudfoot, J. Valacich, G.M. Grimes, and J.F. Nunamaker Jr, "Sleight of hand: Identifying concealed information by monitoring mouse-cursor movements," Journal of the Association for Information Systems, 2019. vol. 20(1).

[13] F. Buisson, Behavioral data analysis with R & Python: Customer-driven data for real business results. 2021, Sebastopol, CA: O'Reilly Media.

[14] M. Loban and A. Yastrebenetsky, Crawl walk run: advancing analytics maturity with Google marketing platform. Second Edition ed. 2021, Austin TX: LionCrest Publishing.

[15] R. Dooley, Friction: The untapped force that can be your most powerful advantage. 2019, New York: McGraw-Hill.

[16] A. Schade. Designing for 5 types of e-commerce shoppers. 2014 [cited 2021 March 2.]; Available from: https://www.nngroup.com/articles/ecommerce-shoppers/.

[17] J. Jenkins and J. Valacich. Behaviorally measuring ease-of-use by analyzing users' mouse cursor movements. in Special Interest Group on Human-Computer Interaction. 2015. Fort Worth, TX.

[18] M. Grimes, J. Jenkins, and J. Valacich. Exploring the effect of arousal and valence on mouse interaction. in International Conference on Information Systems. 2013. Milan, Italy.

[19] M. Grimes and J. Valacich. Mind over mouse: The effect of cognitive load on mouse movement behavior. in International Conference on Information Systems. 2015. Fort Worth, TX.

[20] M. Hibbeln, J.L. Jenkins, C. Schneider, J.S. Valacich, and M. Weinmann. Investigating the effect of insurance fraud on mouse usage in human-computer interactions. in International Conference on Information Systems. 2014. Auckland, New Zealand: Association for Information Systems.

[21] G.M. Grimes, J.L. Jenkins, and J.S. Valacich. Assessing credibility by monitoring changes in typing behavior: The keystroke dynamics deception detection model. in Hawaii International Conference on Computer and Systems Sciences, Symposium on Rapid Screening Technologies, Deception Detection and Credibility Assessment. 2013. Maui, Hawaii.

[22] J.L. Jenkins, J.S. Valacich, and P.A. Williams. Human-computer interaction movement indicators of response biases in online surveys. in International Conference on Information Systems. 2018. Seoul, Korea.

[23] J.L. Jenkins, B.B. Anderson, A. Vance, C.B. Kirwan, and D. Eargle, "More harm than good? How messages that interrupt can make us vulnerable," Information Systems Research, 2016. vol. 27(4): p. 880-896.

[24] J.L. Jenkins, M. Grimes, J.G. Proudfoot, and P.B. Lowry, "Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals," Information Technology for Development, 2014. vol. 20(2): p. 196-213.

[25] J.R. Young, R.S. Davies, J.L. Jenkins, and I. Pfleger, "Keystroke dynamics: establishing keyprints to verify users in online courses," Computers in the Schools, 2019. vol. 36(1): p. 48-68.

[26] J.B. Freeman and N. Ambady, "MouseTracker: Software for studying real-time mental processing using a computer mouse-tracking method," Behavior Research Methods, 2010. vol. 42(1): p. 226-241.

[27] P.M. Fitts, "The information capacity of the human motor system in controlling the amplitude of movement," Journal of Experimental Psychology, 1954. vol. 47(6): p. 381–391.

[28] D.E. Meyer, R.A. Abrams, S. Kornblum, C.E. Wright, and J. Keith Smith, "Optimality in human motor performance: ideal control of rapid aimed movements," Psychological Review, 1988. vol. 95(3): p. 340-370.

[29] O. Hamdy and I. Traoré, "Homogeneous physio-behavioral visual and mouse-based biometric," ACM Transactions on Computer-Human Interaction, 2011. vol. 18(3): p. 1-30.

[30] T.N. Welsh and D. Elliott, "Movement trajectories in the presence of a distracting stimulus: Evidence for a response activation model of selective reaching," The Quarterly Journal of Experimental Psychology, 2004. vol. 57(6): p. 1031-1057.

[31] J.-H. Song and K. Nakayama, "Role of focal attention on latencies and trajectories of visually guided manual pointing," Journal of Vision, 2006. vol. 6(9): p. 11-11.