LuxLeak: Capturing Computing Activity Using Smart Device Ambient Light Sensors

Ashton Holmes
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8281
Los Angeles, USA
ashton.holmes.64@my.csun.edu

Sunny Desai
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8281
Los Angeles, USA
sunny.desai.92@my.csun.edu

Ani Nahapetian
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8281
Los Angeles, USA
ani@csun.edu

ABSTRACT

In this paper, we consider side-channel mechanisms, specifically using smart device ambient light sensors, to capture information about user computing activity. We distinguish keyboard keystrokes using only the ambient light sensor readings from a smart watch worn on the user's non-dominant hand. Additionally, we investigate the feasibility of capturing screen emanations for determining user browser usage patterns. The experimental results expose privacy and security risks, as well as the potential for new mobile user interfaces and applications.

General Terms

Experimentation, Security.

Keywords

Mobile malware, mobile security, privacy, side-channel analysis, smart phone, smart watch, eavesdropping, ambient light sensor, lux, screen emanations, wearable computing.

1. INTRODUCTION

The variety and sensitivity of sensors on smart watches and smart phones has opened up both new possibilities and new security and privacy vulnerabilities. In this paper, we consider the ambient light sensor for the purposes of capturing user computing activity. We specifically look at the effectiveness with which the ambient light sensor can allow applications and/or attackers to capture the keystrokes and the browsing activity of a user working on a computer.

SMARTOBJECTS'16, October 03-07, 2016, New York City, NY, USA
© 2016 ACM. ISBN 978-1-4503-4254-4/16/10…$15.00
DOI: http://dx.doi.org/10.1145/2980147.2980150

This can enable new application possibilities, including allowing blind users to monitor screen information and enable smart watch users to capture keyboard activity without accessing to the computer where the data is being entered.

Unfortunately, the ambient light sensors, if accessed by simple malware, can also be used to violate user privacy by eavesdropping on the user's computing activity.

In fact, this paper expands the currently known security weaknesses inherent in the availability powerful sensors on mobile devices. This is especially pernicious considering the deeply pervasive access that mobile phones commonly have in user lives.

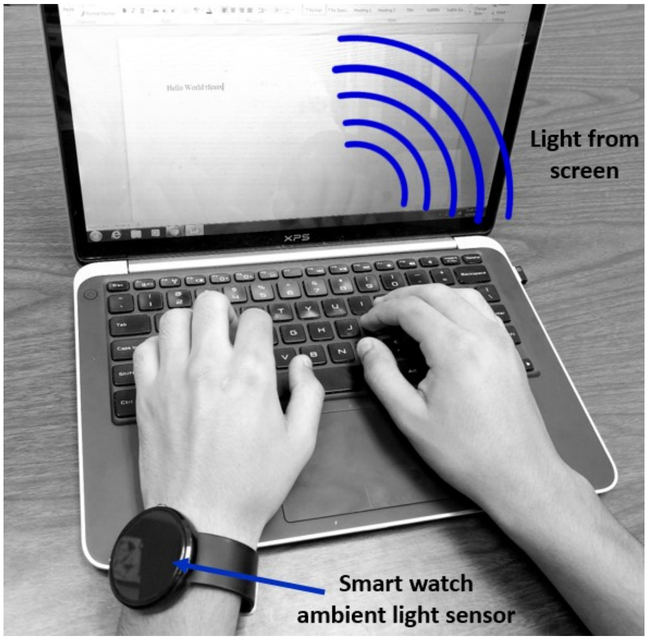


Figure 1. LuxLeak attack model overview, where smart device ambient light sensors are used for capturing screen emanations for monitoring computing activity.

As summarized in Figure 1, we examine the quantity and accuracy of computing activity data (i.e. what you are typing on a keyboard and what you are reading on the web) collected via (malicious) software on a mobile device worn on the user's wrist or placed adjacent to the user.

The paper focuses on a sensor readily available on most mobile devices, namely the ambient light sensor, for the recovery of users' adjacent computer usage activity with screen emanation sensing.

A series of experiments are carried out to the determine the accuracy and precision with which keystrokes on a laptop can be determined, just by measuring the changes in ambient light caused by the subtle movements of the user's wrist towards and away from the laptop screen. Similarly, experiments are carried out regarding the differences in light emanations from different websites, as registered by a smart device placed adjacent to the screen.

To the best of our knowledge, this is the first investigation of using mobile device ambient light sensors for eavesdropping.

2. RELATED WORK

Smart watches and smart phones are equipped with a variety of sensors that have long been leveraged for activity classification, gestures recognition, and keystroke detection. Specifically in terms of keystroke detection cameras, microphones, and motion sensors (including accelerometers and gyroscopes) have been used, with a comprehensive survey provided in [1].

In terms of using smart phones being placed next to a computer for the purposes of eavesdropping, researchers have looked at using the accelerometer to detect vibrations caused by typing as registered by an adjacent phone [2]. Similarly, researchers have looked at capturing sound emanations from keystrokes [3].

Smart watches motion sensors have been used for smart phone numeric keystroke classification [4][5] and keyboard keystroke classification [6].

Ambient light sensors has previously been considered for body position classification [7] and indoor/outdoor detection for the purpose of connectivity optimization [8]. In this work, for the first time, we determine the effectiveness of using the ambient light sensors for extracting computing activity.

3. AMBIENT LIGHT SENSORS

Ambient light sensors are ubiquitous in smart phones and tablets, and they are commonly available on high-end smart watches and wrist-worn activity trackers, including SONY Smart Watch 3, Samsung Gear S, Moto 360 Sport, and FitBit Blaze. The light sensors are typically photodiodes, whose generated current increases under brighter lighting. They are ostensibly used for dimming the screen according to the light conditions, to improve screen visibility and conserve battery power. Differences between cloudy and sunny days, as well as indoor versus outdoor conditions, is readily determined. Figure 2 demonstrates the positioning of the sensor on three different smart watch models available on the market today.

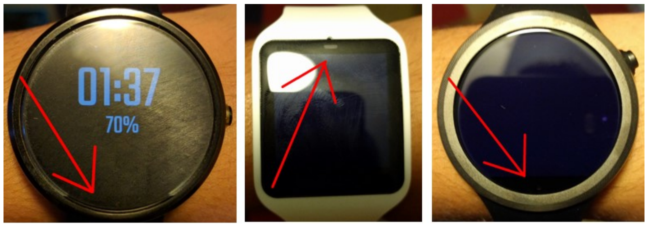


Figure 2. Identification of smart watch ambient light sensor location, for three commercially available smart watches (Moto360 1st Generation, Sony 3, and Moto360 Sport, from left to right).

Light sensors readings, in unit lux (lx), give the luminance per unit area.

The distance of the sensors from the light source impacts the reading. As shown in Figure 3 and Figure 4, increased distance from the computer screen, given in centimeters, clearly impacts the lux readings. The tests shown in Figures 3 and 4 were started at 0 cm from the screen and extended back to 30 cm from the screen over a 30 second time period. The tests, averaged over three runs, were carried out in a completely dark room with only a white screen providing light. Figure 3 gives the lux readings with the smart watch screen facing the screen. Figure 4 gives the lux reading with the smart watch screen perpendicular to the screen, as is commonly expected during keyboard usage. The results of the tests suggest that the ambient light sensor can be used to determine the hand position relative to the screen.

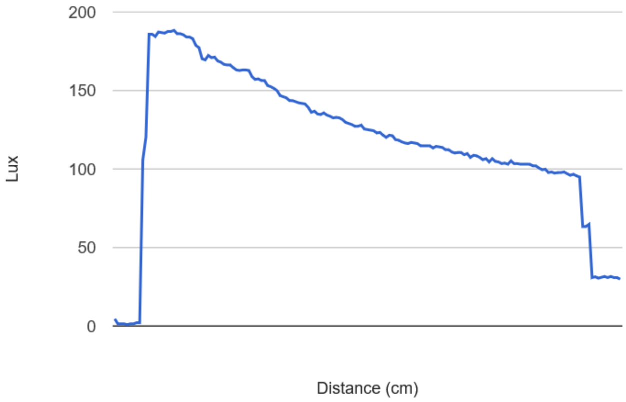


Figure 3. Lux values as distance from screen is increased 1 cm per second for 30 seconds, averaged over 3 runs. The Moto360 smart watch was used with the watch positioned with its face pointing to the screen.

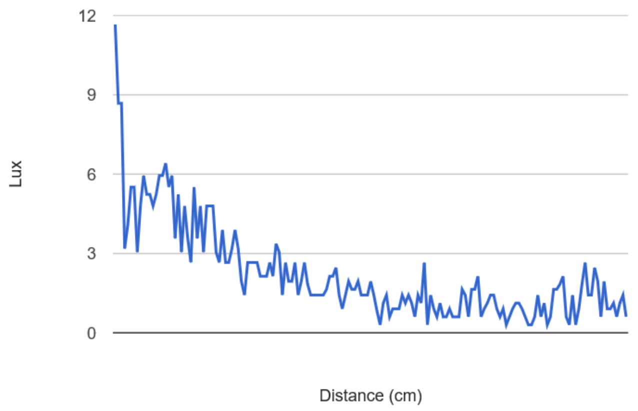


Figure 4. Lux values as distance from screen is increased 1 cm per second for 30 seconds, averaged over 3 runs. The Moto360 smart watch was positioned with its face perpendicular to the screen.

4. KEYSTOKE DETECTION

Consider the scenario and attack model where the user is wearing a smart watch with an ambient light sensor, while typing on a computer with a laptop or desktop keyboard. We investigate the accuracy with which an application or an attacker can determine the keystrokes and hence the information being typed on the keyboard.

An attacker can use this information to limit the search space for a password, determine Google search entries, infer a website being visited, and/or the language being typed.

As the smart watch is typically worn only on the non-dominant hand, language constructs and linguistic knowledge will have to make up for the missed characters entered by the dominant hand.

5. EXPERIMENTAL SET-UP

A series of experiments were carried out to determine the feasibility and accuracy of using smart watch ambient light sensors to determined keystrokes on a computer keyboard.

The experimentation was carried out in a dark room with limited to no outside light. The laptop screen was the main source of light in the room, with the screen set to full brightness.

A Moto360 first generation smart watch running Android 5.1, paired with a Nexus 5X smart phone running Android 6.0, was worn by a right-handed user, on the user's non-dominant left hand with the screen facing up.

Keys were typed on a Dell XPS laptop with a 15 inch screen and a backlit keyboard, running Linux Debian 8.

To carry out the experimentation, each character was typed one character per second for 10 seconds. Then the hands were rested at the home keys for 10 seconds, with the character being typed again once per second for 10 seconds. This test was repeated 3 times, for each character. In other words, there were 20 key presses per test with 3 tests per character, giving a total of 60 key presses per character. All the experiments were conducted across different 3 days.

Resting the hands at the home keys, involves placing the index fingers at the keys 'F' and 'J', without pressing any keys.

The reason the hands were rested on the home keys is two-fold. First, we wanted to move the hand around the keyboard to replicate actual keyboard use. Second, the resting data was used to determine the effectiveness of distinguishing a key press from a non-key press.

All the number keys were typed by the left hand. The letters typed were all those on the left side of a standard QWERTY keyboard. The left shift key and the space bar were also included in the experiments. The shift key provides insight into the keys being typed by the right hand, especially when the space bar is entered by the right hand.

In terms of sample rate, SENSOR_DELAY_FASTEST, which uses 0 microseconds of delay between data pulls was used. Varying the sample rate will clearly affect the accuracy of the results.

6. EXPERIMENTAL RESULTS

Figure 5 and Figure 6 give the scatter plots for the lux readings for typing the number '9' and the letter 'D'. As noted in the previous section, the first 10 seconds are where the character is being typed. During the second 10 seconds the hands are not typing and are at rest on the home keys. During the third 10 seconds the hands are again typing the character.

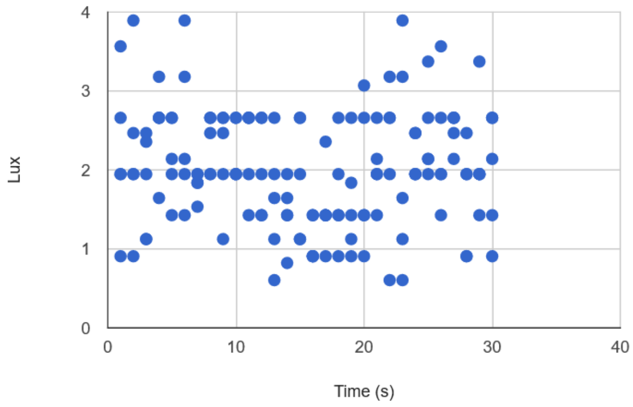


Figure 5. Scatter plot of the lux readings for the number '9'. The 1st 10 seconds and 3rd 10 seconds show the readings as the number is being typed. The 2nd 10 seconds show the readings as the hand returns to the home keys.

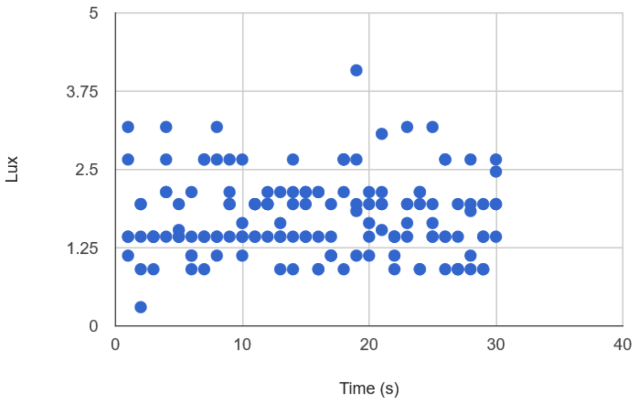


Figure 6. Scatter plot of the lux reading values for the letter 'D'. The 1st 10 seconds and 3rd 10 seconds show the readings as the number is being typed. The 2nd 10 seconds show the readings as the hand returns to the home keys.

As can be seen from the comparison of Figure 5 and Figure 6, the letter 'D' (which is part of the home keys) shows only a small difference between the typing activity and the rest activity. In other words, the lux readings are similar when the hands are resting at D and typing D.

However, with the number '9', there is a difference in the values registered when the number is being typed and when the hands are at rest at the home keys (which do not include the number '9').

Figure 7 provides the average lux readings registered by the smart watch ambient light sensor during all the number key presses. The standard deviation of the readings is provided by the error bars. The readings clearly increase as the hand moves from the left side of the keyboard to the right side of the keyboard. This is expected as the smart watch screen faces the laptop screen when the hand is positioned to press the numbers on the right side of the keyboard. Figure 8 provides the same data, but for the letters, space bar, and left shift key.

Figure 9 provides the heat map of all of the characters, including the numbers, letters, space bar, and left shift key, entered on the keyboard in our experimentation. In the heat map, red represents higher readings than orange, and so on, with green reflecting the lowest lux readings. As the heat map demonstrates, the numbers are clearly distinguishable from the rest of the characters, with their higher lux readings. Similarly, the letters closer to the left edge of the keyboard have lower lux readings. This is again expected, as the face of the watch would face away from the screen as these letters are being entered. Finally, the letters 'C' and 'V' have the lowest average readings, since the palm of the hand, and hence the back of the smart watch screen, are almost parallel with the screen when those letters are typed.

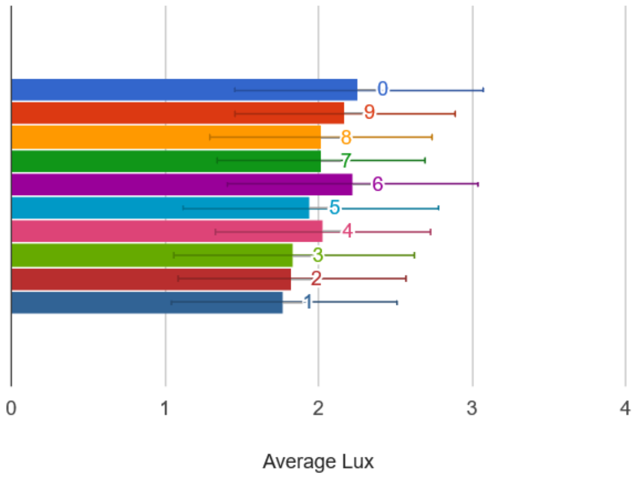


Figure 7. Average lux readings registered by smart watch ambient light sensor for numbers, along with bars demonstrating the standard deviation of the readings.

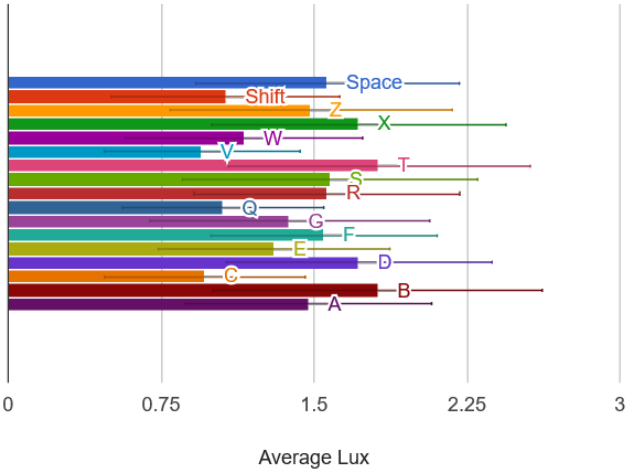
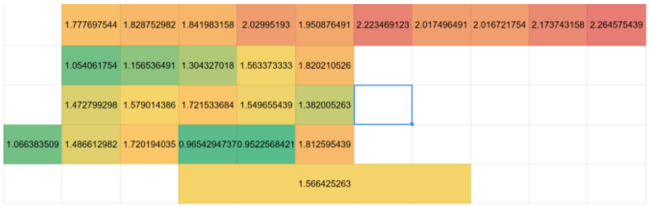


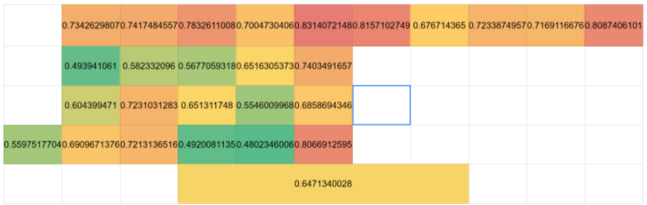
Figure 8. Average readings and standard deviation of lux values collected for the letters, space bar, and shift key; along with bars demonstrating the standard deviation of the readings.

Figure 10 provides the heat map of the standard deviation of the lux readings. It is interesting that the higher lux averages are correlated with higher standard deviation in the readings.



	1.777697544	1.828752982	1.841983158	2.02995193	1.950876491	2.223469123	2.017496491	2.016721754	2.173743158	2.264575439
	1.054061754	1.156536491	1.304327018	1.563373333	1.820210526					
	1.472799298	1.579014386	1.721533684	1.549655439	1.382005263					
1.066383509	1.486612982	1.720194035	0.9654294737	0.9522568421	1.812595439					
			1.566425263							

Figure 9. Heat map of the average lux readings for the numbers, letters, space bar, and left shift key. Colors reflect lux value, with red being larger and green being smaller.

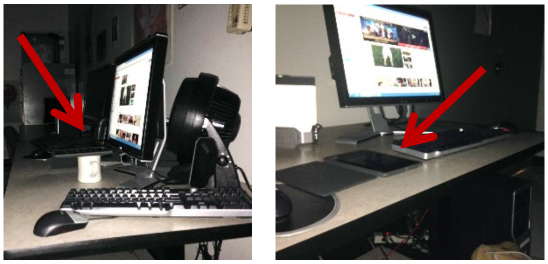


	0.7342629807	0.7417484557	0.7832611008	0.7004730406	0.8314072148	0.8157102749	0.676714365	0.7233874957	0.7169116676	0.8087406101
	0.493941061	0.582332096	0.5677059318	0.6516305373	0.7403491657					
	0.604399471	0.7231031283	0.651311748	0.5546009968	0.6858694346					
0.5597517704	0.6909671376	0.7213136516	0.4920081135	0.4802346006	0.8066912595					
			0.6471340028							

Figure 10. Heat map of the lux reading standard deviation for numbers, letters, space bar, and left shift key. Colors reflect lux value, with red being larger and green being smaller.

7. COMPUTING ACTIVITY DETECTION

In this section, we investigate whether screen emanations captured by smart device ambient light sensors can be used to determine user web browsing activity. Ten popular websites, including YouTube and Gmail, are considered in the experimentation. An Android app is developed to determine the accuracy with which the lux readings can be used to predict the website a user is visiting.



(a) (b)

Figure 11. Experimental setup for monitoring browsing activity using ambient light sensors; with (a) the tablet placed on a 10cm platform centered in front of the screen; and (b) the tablet placed on the table to the left of the screen.

The experimental set-up is shown in Figure 11. Two different set-ups were used. First, the tablet was placed on a 10 cm platform centered in front of the computer monitor. Second, the tablet was placed face up on a desk left of the computer monitor.

The data was collected in a fully darkened room with the DELL PC screen light as the only source of illumination. The ambient light sensor of a Nexus 7 tablet running Android 4.4 was used for capturing the lux readings. Each set-up collected data for a period of one minute, with the SENSOR_DELAY_FASTEST sampling setting.

For each of the experimental set-ups, i.e. elevated or left of the screen, two further variations were considered. First, the average lux values were collected for when the computer monitor displayed the homepage of the website. Second, the average lux readings were collected when the page down key (to move further down the website) was pressed once before recording the lux readings.

Table 1 provides the average lux readings and the standard deviation of the results from the data collection.

The readings from the elevated set-up, where the tablet was centered and raised to nearly the level of the screen are significantly better. Although, smart phones and tablets are more likely to be placed on a table adjacent to the computer screen, smart watches worn by the user during keyboard use are closer to the screen and hence would register more lux information.

The results from the classification of these 10 popular websites is promising. A simple comparison of the lux readings with a prerecorded average website lux value is sufficient to distinguish the web browsing activity of the user, using only a smart device's ambient light sensor.

8. CONCLUSION

In this paper, we presented a series of experimental results that considered the effectiveness with which a smart device's ambient light sensor can be used to monitor user computing activity, namely keystrokes on a keyboard and web browsing activity. In the case of smart watches, light emanations from the computer screen are used to determine the distance of the wrist from the screen, and hence the keys being pressed. Additionally, the average light values and variations registered by a mobile device are used to determine the website a user has up on the computer screen. The results demonstrate the security vulnerabilities and the user interface possibilities of the often overlooked ambient light sensor are more significant than originally perceived.

9. REFERENCES

[1] Ani Nahapetian. Side-Channel Attacks on Mobile and Wearable Systems. *IEEE Conference Consumer Communications and Networking (CCNC)*, January 2016.

[2] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*.

[3] Yigael Berger, Avishai Wool, and Arie Yeredor. 2006. Dictionary attacks using keyboard acoustic emanations. In *Proceedings of the 13th ACM conference on Computer and communications security* (CCS '06).

[4] Allen Sarkisyan, Ryan Debbiny, Ani Nahapetian. WristSnoop: Smartphone PINs Prediction using Smartwatch Motion Sensors. *IEEE Workshop on Information Forensics and Security (WIFS)*, November 2015.

[5] Anindya Maiti, Murtuza Jadliwala, Jibo He, Igor Bilogrevic. (Smart)watch your taps: side-channel keystroke inference attacks using smartwatches. In *Proceedings of the ACM Internationl Symposium on Wearable Computing (ISWC)*, September 2015, 27-30.

[6] He Wang, Ted Tsung-Te Lai, and Romit Roy Choudhury. 2015. MoLe: Motion Leaks through Smartwatch Sensors. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking* (MobiCom '15).

[7] Arsen Papisyan, Ani Nahapetian. LightVest: A Wearable Body Position Monitor Using Ambient and Infrared Light. *ACM International Conference on Body Area Networks (BodyNets)*, September 2014.

[8] Pengfei Zhou, Yuanqing Zheng, Zhenjiang Li, Mo Li, and Guobin Shen. 2012. IODetector: a generic service for indoor outdoor detection. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems* (SenSys '12).

Table 1. Average lux values (lx) and standard deviation for ambient light sensor readings across 4 different experimental set-ups for 10 popular websites.

Setup	YouTube	Twitter	Tumblr	Gmail	Facebook	Amazon	Wikipedia	Google	Yahoo	eBay
Elevated	20.9847, 2.7206	34.2444, 2.6185	13.6990, 2.3881	32.4649, 2.6091	28.8918, 1.9763	28.5638, 1.9419	31.0806, 2.6597	34.6453, 2.6734	18.6063, 2.3489	15.6806, 2.3978
Elevated, Page Down	21.7827, 2.5985	34.6312, 2.5433	7.8442, 2.2292	32.6678, 2.6702	30.1597, 2.4913	33.1120, 1.9875	33.2917, 2.6436	34.6453, 2.6734	30.5259, 2.4631	24.4727, 2.4665
Left of Screen	1.3507, 1.2647	1.7088, 1.3977	1.0417, 1.0455	2.6738, 0.9470	1.3881, 1.3010	1.3118, 1.2406	2.0998, 1.8028	1.5420, 1.3593	1.2697, 1.2238	1.2552, 1.2010
Left of Screen, Page down	2.0561, 1.7838	1.6740, 1.3940	1.0000, 1.0074	2.1024, 1.7854	1.4971, 1.3537	1.3650, 1.2865	1.4987, 1.3261	1.5420, 1.3593	1.1349, 1.1421	1.1382, 1.1308