Designing for Vigilance during Intermittent Use

M. Giles Phillips
subforum.org
PO Box 130451
Boston, MA 02113
giles@alum.mit.edu

ABSTRACT
Internet usage is shifting towards a persistent and pervasive engagement through connected mobile devices. In Social Media, this engagement is mediated by an online profile, through which our interactions with online social worlds are framed. By adapting and mediating the embodied acts of Identify Performance and Impression Management, the online profile informs socialization and self-identity. This research posits that the particular use case for maintaining an online profile creates an unprecedented, technology-driven form of human vigilance during intermittent use. Scholarship into the nature of online profiles will be examined, as well as the instinctual basis for human vigilance. A review of Human Factors (HF) research concerning vigilance, and the Human-Computer Interactions (HCI) that support vigilance today, are also provided. A set of design principles is subsequently proposed in order to guide the design of more effective and sustainable interactions that support vigilance during cases of intermittent use. These principles can be generalized from social networking into numerous domains of HCI.

Categories and Subject Descriptors
H.1.2 [Information Systems]: User/Machine Systems - human factors, human information processing, software psychology.
H.4.3 [Information Systems Applications]: Communications Applications - information browsers.
H.5.0 [Information Interfaces and Presentation]: General

General Terms
Design, Human Factors, Theory.

Keywords
Vigilance, Intermittent Use, Social Media, Mobile.

1. INTRODUCTION
Vigilance is typically something that we associate with an external force or threat: a herdsman watching over his sheep; anesthesiologist monitoring her patient’s vital signs; security scanning passengers at the airport. Our motivation to be watchful is rooted in the potentially grave consequences of not paying attention: the loss of some of the flock; the patient going into failure; a terrorist attack. Vigilance in the use of Information Systems is a scenario for an expert user who is being watchful for a discrete set of cues that might require him to take action.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 2012 ACM 978-1-4503-1228-8… $10.00.

Various forms of user vigilance have been examined since World War II, when researchers began examining the alertness of Radar System operators. [10,11] The radar operator and his unique form of vigilance emerged because technological innovation enabled new types of information to be captured. Similarly in today’s world, 3 key technological factors have led to the emergence of a new type of vigilance, on a much broader scale: the explosion of content generated in virtual experiences, an increase in content’s personal importance, and massive growth in mobile device usage.

Connected mobile devices extend our bodies, [3] providing new signals to sense: texts, social updates, news, and so on. These signals are seductive. They provide insight into what’s happening in the bigger world around us. But if one wants to stay on top of these fleeting communiqués, one must watch for them. This has created a crisis of attention, particularly in the social realm. [3]

Our urge to socialize is instinctual, but the mechanisms and tactics for socializing are learned and can change. In social media systems, interaction is mediated through an online profile, and users learn to socialize through this profile. In so doing, the socialization processes that used to occur only during direct human interaction are partially shifted into mediated experiences. When socialization processes are made thus exogenous, the individual must watch over developments in these mediated experiences, in order to avoid the dissocializing effects of not paying attention. This watchfulness over the exogenous self is an unprecedented, technology-driven form of human vigilance.

2. VIGILANCE IN SOCIAL MEDIA
Historically, it hasn’t made sense to talk about vigilance as part of how we socialize. Socialization is a naturally embodied and immediate process, guided by instinct, personality, observation, and conditioning, but not vigilance. But social networks change our social landscape by providing external mechanisms to facilitate Identity Performance. [1] Identity Performance is done instinctually: it’s a process for understanding how others perceive us. [1] Imagine that you’re a high school student, making a sarcastic statement to a new classmate about your math teacher. You feel this statement represents you in a certain light, so you watch how your classmate reacts. What does he say in response? Does he change his body language or make a face? Based upon your observations, you begin to flesh out your ideas about your classmate, and you may modify or experiment with your behavior.

This act, known as Impression Management, encapsulates Identity Performance in a looped process: you perform some action, you observe the impact of that action, and you learn. [1,6] You don’t think about this consciously—it’s an invertebrate element of human interaction and over time it supports the development of a more nuanced view of people, and your own sense of self-identity. The process of Identity Performance is cyclical and perpetual: we use it to develop social skills and to socialize over our entire lifetime, particularly during our teenage years. [1]

369
As a form of public, online networks uniquely impact the acts of Impression Management and Identity Performance. [2] First, our interactions in these networks are generally remembered by the system; they persist. Traces of our interactions can linger on for quite some time, and are discoverable to groups of people at different times. Moreover, we don’t always know specifically who might be online when we communicate, or even comprehend the size of the audience for our communications over time. This is partially due to the persistence of the data in the network, and partially due to the intransigence of the scope of our communications: it’s hard to get a sense of the size and reach of things we say. When we say or do something, we’re actually addressing an imagined audience that may or may not correlate with our true, actual audience. [2]

These characteristics of networked publics are designed abstractions of human interaction. Together, they mean that people must develop a new set of skills for Identity Performance. [1] A first-time or novice user of the system must initially become familiar with the rules of the network, and the different ways that she can project her sense of self into the network. Over time, she develops an expert understanding of the facets of her online identity – how many connections she has, what her profile picture suggests about her, how people react when she does certain things, and so on. She also develops a more solid conceptual model of how all of these facets facilitate Identity Performance. The fact that social media externalizes specific social mechanisms from her embodied experience doesn’t stop her from doing Identity Performance; rather, it means that she must watch over her social networks to understand the impacts of her actions. Her vigilance thus emerges:

2.1 The Online Profile Informs Self-Identity
An online profile is often thought of as a simple representation of 1 or n dimensions of our physical selves. It is something we control, something we own. Yet for many, and particularly those individuals who discovered social networks in their formative years, the relationship is different. [2,3] Socialization via their online personas is an essential part of their identity; in fact, it’s a fundamental component to how they learned to socialize. Their profile partially defines them. [3] Their network interactions facilitate cyclical acts of Identity Performance exogenously; these acts become core to the individual’s sense of self.

2.2 Impression Management Takes Vigilance
Because it is exogenous, the social network next needs to be monitored, in order to sustain Impression Management through the online profile. This is the obvious thing about externalized, online Identity Performance: it can be less immediate. It’s disembodied. There is asynchrony. When I communicate, I can’t always rely upon any form of immediacy in terms of a response from my audience. They may not be online, or they may not be paying attention at that moment, but my communications persist. So in order to perform Impression Management - to understand the effect of my communications - I have to repeatedly and actively check on the network. This basic “take action, observe the consequence” loop is stretched over an indefinite period of time. Fundamentally, once the individual gets his profile set up in the network, he has to watch over it in order to understand how he fits in. This is the basic urge that drives vigilant use.

2.3 Touch Points are Identified
Once the user feels the need to be watchful of developments in the network, he begins to recognize all of the touch points in his routine navigation of the physical world that he can create in order to manage the watching. Dad starts logging in on his smart phone during downtime throughout the day. Mom begins logging in while she watches TV. Their son is logging in while he drives. Each is checking for new developments that require action.

3. THE DRIVERS OF VIGILANCE
Essentially, vigilance is about an individual preserving her well-being, or the well-being of those who are under her care, or those that she cares about. Through the observation of flocking birds and herding groups of mammals, we’ve established that the amount of energy an individual focuses upon vigilance is inversely related to the size of that individual’s group. [15,9] The larger the size of the community or group of animals, the less vigilant any individual animal will be. Individuals situated along the periphery of the group will tend to be more vigilant than those in the middle of the pack. [9] This suggests that vigilance is instinctually contextual, and it makes intuitive sense: if you’re along the edge of the herd you’re more likely to be a target.

But interestingly, the most vigilant individuals in the herd must still divide their attention – the individual along the edge of the herd must sustain vigilance while also trying to eat. This scenario illuminates a few critically important dimensions of vigilance that are reflected in today’s mediated worlds. For one, even though the peripheral grazers are eating instead of paying full attention to their watch, they are still able to note and react to the threats. [9] This suggests that some amount of attention is constantly dedicated to vigilance and also that multiple senses are used to be vigilant. Even though the animals are most vigilant while sustaining their watch, they can be sufficiently vigilant while grazing. This also means that vigilance is comprised of bouts of watchfulness; it is not necessarily sustained watchfulness. [9] Vigilant grazers are multitasking: sustaining some amount of attention to vigilance while eating.

The social media use case is similar; an active social networker isn’t always looking. He may intermittently check on the network throughout the day, via his smartphone, but for big chunks of his day the smartphone is likely stuffed in his pocket. The signals or cues that prompt a vigilant user to check on the status of the network are one of two things:

- Exogenous cueing: signals in the form of an alert or notification from their device
- Endogenous cueing: the user’s internal, instinctual cycle of Identity Performance; specifically, where the user is engaged in Impression Management

Stated another way, an attentive Twitter user will check his phone either when it buzzes at him, or to see if anyone has responded to his tweet. The vigilant user thus sustains some amount of attention to the monitoring of his network for exogenous cues, even during periods of time where he is not actively using the network. Vigilance is not always a case of sustained, focused use of an interface; it can also be a case of sustained awareness and occasional use.

4. VIGILANCE IN HCI
As technology has become increasingly sophisticated, we have naturally applied technology to extend our senses and facilitate increased vigilance. Technology provides an extension to our embodied ability to sense: amplifying or translating signals, or providing new signals, so that we can react. As such, vigilance in information systems is concerned with a user’s attention, focus, and ability to detect signals. [11] Vigilance has classically been considered one of three types of attention: [11]
• Vigilant (sustained) attention: continuous allocation of processing resources
• Divided attention: simultaneously monitoring multiple sensory channels
• Selective (focused) attention: monitoring some sensory channels and ignoring others

Vigilance is a uniquely taxing state; it consumes time and attention, and it’s exhausting. [17] A known phenomenon is the vigilance decrement, which is the tendency of people to overlook or misinterpret signals increasingly over time. [10] The vigilance decrement correlates either to a decrease in the user’s physiological sensitivity (i.e. through habituation), or to a change in the user’s decision criteria (i.e. her evolving perspective on how consequential she believes the signal to be.) [11,12] Tactics for reducing the vigilance decrement include increasing the salience of signals, lowering the event rate of signals, and if possible, inserting false signals. [11]

Classically, vigilance has been associated with sustained use cases like radar operation, air traffic control, and anesthesiology. [11,12] Prior to the emergence of mobile connectivity, it was safe to assume that vigilant attention would be associated with sustained use, because often as not, usage meant you were glued to a desk. Mobile connectivity has changed that: vigilance is now sustained over bouts of intermittent use in information systems. Thus in order to account for every vigilance scenario in HCI, including the emergent use case in social media, our definition of vigilance must be extended to include intermittent use.

4.1 Baseline Conditioning
Vigilance is predicated upon our ability to recognize and evaluate the normalcy of a healthy scenario: a baseline condition. Information systems enable vigilance first by giving the user a sense of what normal looks, feels, or sounds like. In visual displays of information like a graphical user interface, this is accomplished by a user’s visual search. [1] Visual search is a perceptual task in which the user actively scans his visual field in search of target objects or features, among a field of other objects or features, known as distractors. [19,18] As users develop expertise within a particular environment or interface, they will begin to operate with a set of preconceptions that help simplify visual search by constraining the visual field or cueing to particular features in the visual field; these preconceptions may create biases when interacting with new environments. [18,7,14]

In today’s world of social media and social computing, the baseline condition is established through use, developing a sense of what’s normal within the Information Architecture (IA) of the product. A social network’s IA often includes: [2]

• An online profile which represents the user.
• Collections of relations, like your list of friends on a social network, or the list of editors of a wiki document.
• Tools for public communication. Messaging, sharing, and activity feed: nuggets of personalized communication.

These features become the lynchpin of the user’s conceptual model for interacting within a social networking site. The foundation of vigilance for the social networker is the scanning of these features in order to verify that the baseline condition is met: does she have any new followers? Did she lose followers after her last tweet? Did her friend reply to her message?

4.2 Alert Flaring
With the baseline condition established, alerts can usually help a vigilant user recognize events that may require her to take action. An alert is any mechanism designed to capture the user’s attention. [2] Effective vigilance requires the ability to quickly differentiate real alarms from false alarms and non-threatening occurrences. A major design consideration is the relative salience of the alert signal in all usage contexts. [18,7] Because loud or persistent alarms can annoy users, the design of alerts must strike the right balance between false alarms and missed events. [18]

Visual alerts are restricted to the user’s visual field, which can be difficult to predict. [18,19] A salient color can be used - as well as flashing and blinking - in order to draw a user’s attention to a particular area in her visual field. [7,18] Other transformations, such as changes in shape or positioning can also be used to signal alerts to the user. [14] Both sound and ergonomic alerts (like tactile vibrations from a mobile phone) can be effective because they are omnidirectional. [3] In some scenarios, visual, audio, and/or ergonomic alerts can be combined to increase salience. [18]

In today’s world of Web and connected devices, visual alerts are commonly invoked through salient visual overlays on top of the User Interface (UI), like a badge over an email icon indicating the number of unread messages. These mechanisms can be effective during sustained use, but also when the user is multitasking and her attention is divided. [20] In both cases, the user conducts a visual search of the UI in order to establish the baseline condition, and if alert overlays are present or emerge near particular features, they can help the user to identify exceptions.

In situations where sustained use cannot be assumed, email is a long-standing and popular alerting mechanism; it is used by most social systems. Email has a number of well-known issues: loss of salience or user desensitization due to the amount of junk and spam that exists in their inbox, messages being caught by spam filters, and no mechanisms for verifying that the email was read.

In mobile operation systems, a notification system is typically included. Such systems are often mixed-mode: visual information is displayed, and the device will correspondingly issue an audio chime and/or an ergonomic vibration. An on-screen dialog is generally provided, which enables the user to ignore the alert or to view/take action. These systems are user-configurable, enabling one to tune the salience and differentiation of signal types, often on the fly. Mobile notifications have helped users divorce some of their attention from their online personas while continuing to be watchful over them. But mobility opens the door to myriad contexts of use: it is impossible to know what else the user might be doing while being vigilant. As more services leverage mobile notifications, the relative salience of any single notification may decrease. Increased adoption introduces the risk of over-saturating users, flooding them with alerts that aren’t important.

5. DESIGNING FOR VIGILANCE
A user sustaining vigilant attention over intermittent use is uniquely impacted. His attention is divided between mediated and physical experiences. Users may be distracted from, or by, their vigilant state. Building upon the established tactics and shifting

_____________________
[1] For a deeper inquiry into visual search, refer to [5,8,13,16,19].
[2] [20, 18] do an excellent job of summarizing the rich body of research into user attention and its application.
[3] Ergonomic alerts are quite effective at getting the user’s attention and can be less annoying than auditory. [18]
our focus to the design of support for vigilance during intermittent use, the following principles are proposed:

1. **Provide a Vigilance Lens.** The vigilance lens should be an expert view that users can naturally flow into when they feel the need to be vigilant, and out of when they’re bored or curious. The vigilance lens must also provide short paths to react: most use cases will conclude with the performance of some action, and this should be made as frictionless as possible. Many social systems today are designed with the opposite goal of keeping users engaged as long as possible, and risk turning vigilance into the gateway for more casual immersion into mediated experiences.

2. **Simplify for Visual Search.** Remembering that the vigilant user will be an expert user who is familiar with your system, ensure that users can easily establish their baseline condition. The baseline condition should provide a clear framework within which to flare alerts. For users entering your system via an alert, you must provide them with sufficient context to act.

3. **Use Intelligent Signal Flaring.** Prioritization and batching can be employed to minimize false positives or the alert of non-meaningful activity. Less important signals can be batched together and cued at once, allowing the user to engage less frequently. Alerts may be overloaded to help users quickly establish context; for example, compressing a sequence of events into a timeline the user can quickly step through without entering your system.

4. **Introduce variance in Signals.** Variance shakes things up and makes the user less likely to dismiss alerts over time, combatting the vigilance decrement. [10,11] For example, consider the tuning of signal salience or timing to correlate with the priority of the alert.

6. **NEXT STEPS**

Future work to further develop this exploration must include research into the applicability of the existing body of HF research of vigilance to this new form of vigilance during intermittent use, including the vigilance decrement and the specific factors that impact it in these systems. Further empirical investigation into user’s specific decision criteria when monitoring alerts is also needed. Finally, the proposed design principles require further development: while they help to frame the problem of designing for vigilance, they are only the beginning of what should be a much deeper inquiry.

7. **CONCLUSION**

We must reconsider the classical notion of vigilance in HCI: technological innovation has introduced a new form of vigilance that extends over periods of intermittent use. While this article explored the particular phenomenon of vigilance among social networkers, it is a much more broad and growing concern, potentially relevant to any real-time analytics or reporting system, publishing system, or home and health monitoring systems. On one hand, this is an opportunity: businesses might relish in the opportunity to have a more broadly engaged audience. But it’s also our responsibility to design products that users can engage with easily, quickly, and in a way that doesn’t disrupt navigation and socialization in the physical world. To support vigilance during intermittent use, we must enable users to be watchful over the developments in our systems with short, efficient workflows. We must also change the way we think about people, how they interact, and how they navigate and occupy physical space.

8. **REFERENCES**


