

---

# An ethical Internet monitoring device enabling child resilience online

**Catherine Flick**

Middlesex University  
The Burroughs  
Hendon, UK NW4 4BT  
c.flick@mdx.ac.uk

**Penny Duquenoy**

Middlesex University  
The Burroughs  
Hendon, UK NW4 4BT  
p.duquenoy@mdx.ac.uk

**Matt Jones**

FIT Lab  
Computer Science  
Swansea University  
always@acm.org

**Nicholas FitzRoy-Dale**

University of New South Wales  
Anzac Parade  
Kensington, NSW, Australia  
nfd@cse.unsw.edu.au

**Basmah Alhodaithi**

FIT Lab  
Computer Science  
Swansea University  
basmah.alhodaithi@gmail.com

**Abstract**

This paper describes a work in progress device that allows for ethical monitoring of children online, fostering discussion in families about internet use and enabling children to become more resilient to potential online predators.

**Keywords**

Monitoring, ethics, surveillance, child protection

**ACM Classification Keywords**

H.5 INFORMATION INTERFACES AND PRESENTATION  
(e.g., HCI); H.5.m MISCELLANEOUS

**General Terms**

Design, human factors, Internet monitoring device, online child protection, ambient display,

**Introduction**

"Ghosty" is a network-enabled monitoring device aimed at encouraging discussion in families about children's internet use. It allows household members to know what types of websites or networks are being visited or used, rather than specifics of particular websites or conversation details. The device shows internet access according to type delineation (such as "homework", "social", "email") by varying the colour shown by LEDs

---

Copyright is held by the author/owner(s).

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.

ACM 978-1-4503-0268-5/11/05.

within a lamp. This is a work in progress at the very early stages, with a basic prototype of the lamp and network monitoring complete. The contribution of this paper is its argument and illustration of a novel approach to helping families negotiate the “dangers” of the internet. Instead of policing, restricting or reporting, the prototype aims to support awareness, reflection and conversation, respecting and drawing on the social, collaborative and complex nature of family life.

### **Background**

Online child protection approaches can be split into two groups: the first being prevention of crimes occurring and the second being the finding, arresting, and prosecuting of offenders. The former has traditionally relied on deterrence (from prosecutions), education of children as to their safety online, and monitoring and/or filtering devices for home and school networks. The latter relies on sophisticated software used by law enforcement for tracking paedophile behavior, such as Peer Precision or the Isis Project [6], as well as traditional policing methods to identify potential abusers and distributors of child sexual abuse material online.

Although the latter approach is useful in apprehending paedophiles, ideally child sexual abuse crimes would be avoided altogether. Thus there is a need for methods and mechanisms for prevention of offences, most of which centre on supervision of children on the internet, such as parental education which suggests that computers should be kept in a public part of the house, or that parents should supervise their children on the internet. Monitoring and filtering tools such as Net

Nanny<sup>1</sup> have also appeared, allowing parents to set limits on internet use, email them on keywords used during a child’s internet session, or block certain pages.

The problems with traditional monitoring and filtering devices are numerous, particularly from an ethical perspective:

- They can cause rebellion in a child which comes up against such filtering or monitoring systems, fostering subversion or other work-arounds of the system;
- They can trigger false positives and block innocent content;
- They can impinge on the privacy of the child, by emailing a parent when a child uses a key word, for example, or simply allowing a parent to view all chat text; and,
- They can cause a child to become more secretive about their behavior online, to name a few.

Social networking has also come into the spotlight in recent times, to the degree that the UK child protection agency CEOP produced a Facebook “emergency button” application for children worried about others’ behavior online. The “ClickCEOP” application<sup>2</sup> allows children to report suspicious activity toward them on Facebook as well as learn about safe internet practices.

Recent research has come to light showing that many children are not at all vulnerable to online predators: these young people who are approached are, in this way, “resilient”, telling potential offenders to go away.

---

<sup>1</sup> <http://www.netnanny.com/>

<sup>2</sup> <http://apps.facebook.com/clickceop/>

However, there is a smaller group of young people, the “disinhibited”, who are often willing to interact with offenders and engage with them due to various reasons, such as negative self-esteem, parental problems, difficulties at school, loneliness, tendency to self-harm, or familial sexual abuse. They can, in some cases, use sexual names or actively seek sexual encounters with people online. These are ideal targets for paedophiles seeking relationships with children with the possibility for future contact offences [1].

In this project, we wish to enable more families to engender a sense of resilience in their children, particularly those who have the potential to slip either way into the disinhibited or the resilient group. Our project also aims to reinforce resilience amongst children who are already resilient, allowing for parents to loosely monitor their internet activity without knowing details, but using this knowledge to spur positive conversation and discussion amongst family members.

In this way the device aims to be an ethical monitoring tool used in a very specific way to enable resilience amongst children and allow for greater family bonds that could help prevent disinhibition.

Our work is further informed by three sets of technology and interaction research and practice. Firstly, there have been a number of devices that attempt to represent internet traffic in ambient and intriguing ways. The first display of this sort was LiveWire, a dangling piece of string that twitched as data packets passed through the server it was connected to [4]. More recently, commercial devices

such as the Nabaztag Rabbit<sup>3</sup> have been successfully marketed. The Rabbit is an electronic Wi-Fi device that was designed to use many interaction techniques. It speaks, listens, moves, whistles, reports and shows hundred of colours and special patterns of light.

The second area of inspiration concerns the approaches to used to nudge energy consumption behaviour within homes. To increase awareness there are many devices that have been developed and studied to provide users with feedback of their energy consumption. Some of these devices provide users immediate and continuous feedback using mobile phones, online visualisation or minimal ambient displays [7]. The PowerAware cord presents energy use as a pulsating flowing, light stream along a powercord to the device being operated. Its developers argue for home devices that promote conversations and provide pleasure over ones that judge or preach behaviour change [2].

Thirdly, we are drawing on previous socio-technical work concerned with building and sustaining cohesive, healthy family living (e.g. [3] [5]).

---

<sup>3</sup> <http://www.nabaztag.com>



Figure 1: "Ghosty", the colour-based internet monitoring device. The device changes colour dynamically to reflect internet use patterns at home.

### **"Ghosty", the ethical internet monitoring device**

The device we have developed is a series of coloured Light Emitting Diodes (LEDs) implanted in a child's ghost-shaped lamp, which, when connected to a computer, change colour depending on the type of network activity on the computer, particularly the types of websites being visited (Figure 1).

There are two parts to the device: the hardware and the software. The hardware is an Arduino chipset into which the LEDs and USB cable are connected. At the moment, power is derived from the USB connection. The LEDs are individual red, green, and blue LEDs, but in the future will be replaced by all-in-one RGB LEDs which will cut down cost and improve the ease of development.

The software is comprised of two parts: the code running on the Arduino, and the software running on the PC being monitored.

The former is a set of simple drivers that run the Arduino chip, allowing a control program on the computer to change the LED colours to specific RGB values.

The latter is a Python program that listens on network sockets and makes decisions based on where the network traffic is coming and going. If, for example, a child is visiting educational, "homework" websites, the lamp may change to green. However, if the child visits a social networking site such as Facebook or Twitter the lamp changes to yellow. Use of email or instant messenger may change the lamp's colour again, and so on. There is also the potential to tailor the lamp's

colour changing to particular sorts of use, for example, instant messenger conversations could be singled out and colour coded depending on the topics of conversation, etc.

The lamp is designed to be placed in a central, social part of the home such as the kitchen or sitting room where a parent could maintain a simple supervision of their children without obtaining too much information other than the sorts of activities any one child is engaging in.

In some ways this would be a little like knowing a child is playing inside (low risk), or in the back yard (low risk), or at a friend's house (low risk), or at the park (higher risk), or at school (low risk), or is running about in the city (high risk) and thus allowing the parent to judge the relative risks and requirements for supervision on that basis. Even if supervision is not required, the knowledge of the general activities of the child on the internet could be used as conversation starters to build family relationships or to discuss online safety measures.

As this is a work in progress, we have not yet progressed past a functional prototype, and have not yet formally engaged any stakeholders. Initial responses from parents of children of internet use age have, though, been extremely positive.

### **Next Steps and Future Goals**

The planned additional work as it progresses includes the following activities:

- further engaging with stakeholders and users, particularly families with young children who use the internet, to elicit their response to the concept;
- exploration of how to usefully categorize and visualize internet activity with stakeholders and family users;
- explore the relative values of dynamic, real-time visualizations over aggregated, longer-term presentations (showing for example internet use over a day or the weekend);
- enabling the device to listen to and visualise a household's activity rather than being tied to one specific computer in the home;
- establishing guidelines for parents to use the device to enable effective discussion and resilience-building; and,
- conduct an ethical analysis of the device, so that it is developed with ethical values at the forefront of the technology.

### **Conclusions**

This work aims to introduce an ethical internet monitoring solution that enables and fosters resilience in children by allowing parents to monitor children in terms of the types of internet activity they participate in yet allows the children to retain their independence and privacy as to the specifics of that activity. It uses colour as an easy way for parents and children to

identify risk and then to determine appropriate levels of supervision for their child.

### **Acknowledgements**

The authors gratefully acknowledge the support of the EPSRC (EP/F035071/1 & EP/F035454/1).

### **Example citations**

- [1] J. Davidson. 2010. Understanding online offending behavior: Preliminary findings from the European Online Grooming Project. *Online Child Protection: Future Technologies for Policing the Internet*. London (2010) <http://european-online-grooming-project.com/>
- [2] Anton Gustafsson and Magnus Gyllensvärd. 2005. The power-aware cord: energy awareness through ambient information display. In *CHI '05 extended abstracts on Human factors in computing systems* (CHI '05). ACM, New York, NY, USA, 1423-1426.
- [3] Andrea Grimes, Desney Tan, and Dan Morris. 2009. Toward technologies that support family reflections on health. In *Proceedings of the ACM 2009 international conference on Supporting group work* (GROUP '09). ACM, New York, NY, USA, 311-320

[4] Hiroshi Ishii and Brygg Ullmer. 1997. Tangible bits: towards seamless interfaces between people, bits and atoms. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '97), Steven Pemberton (Ed.). ACM, New York, NY, USA, 234-241.

[5] Alex S. Taylor and Laurel Swan. 2005. Artful systems in the home. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '05). ACM, New York, NY, USA, 641-650

[6] Patrick G. Watson, Penny Duquenoy, Margaret Brennan, Matt Jones, and James Walkerdine. 2009. Towards an ethical interaction design: the issue of including stakeholders in law-enforcement software development. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7* (OZCHI '09). ACM, New York, NY, USA, 313-316.

[7] Tae-Jung Yun. 2009. Investigating the impact of a minimalist in-home energy consumption display. In *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems* (CHI '09). ACM, New York, NY, USA, 4417-4422.