

Chapter 14

Effective, Privacy–First Display Advertising: Ambient Intelligence for Online Ambient Environments

Ratko Orlandic
Gorsel, Inc., USA

ABSTRACT

This chapter addresses the problem of architecting display ad networks for online social media. The basic question behind this work is: Can display advertising in social media be effective while providing rigorous privacy guarantees? The chapter exposes the problems that display advertising faces in social media, introduces a display ad-network architecture organized around the goals of effectiveness and privacy enforcement, and describes a type of social media for which the architecture is ideally suited. To deliver high effectiveness in a social media environment, the ad network must function as an embedded component of the environment with ambient intelligence. Moreover, the architecture must constrain data and mechanisms in order to deliver rigorous privacy guarantees as a baseline and an additional set of choices to enforce even stricter views on privacy. Ambient social media sites, described later in the chapter, are the most appropriate form of social media for the proposed architecture.

INTRODUCTION

Computational advertising (Anagnostopoulos, Broder, Gabrilovich, Josifovski, & Riedel, 2007; Choi et al., 2010; Yan et al., 2009) has been one of the main forces behind the success of Web. As long as users appear on Web in increasing numbers and the investment into online marketing grows, Web will continue to be a place of growth and innovation. To keep the process going, online advertising should maximize the synergy of factors that contribute to the effectiveness of ad serving, while minimizing factors detrimental to response.

DOI: 10.4018/978-1-5225-8897-9.ch014

Privacy is another major concern of contemporary data analysis (Dwork, 2011), including computational advertising. Information about the user or the user's Web behavior can be intrusive. So can the data derived from privately-generated content. Despite some tension between response and privacy goals, rigorous privacy enforcement is not only conducive to higher response but an important pre-requisite for it. Anything less deters users from clicking on ads.

In online display advertising, ad exposures appear within or next-to the displayed Web page. This form of advertising has become the main revenue generator for publishing media (Lee, 2012). The relative success of online display advertising and the explosive growth of online social media (Bakshy, Rosenn, Marlow, & Adamic, 2012; Park, Lee, Kim, & Chung, 2013; Sang & Hu, 2013) have fueled the expectations that display advertising can be just as advantageous in online social media settings. However, an integration of display advertising in social media requires a full awareness of potentially ensuing problems.

In this paper, we pursue the design of ad networks for online display advertising in social media environments. Whether and where in online social media can such advertising be effective and adhering to strict privacy constraints is the question that motivates this work. We will not pursue a universal solution for all kinds of social media, but one that can deliver high effectiveness in types of social media that facilitate the goals of effectiveness and privacy enforcement. The paper exposes the problems that display advertising faces in social media, presents a display ad-network architecture organized around the two goals, and describes a type of social media for which the architecture is ideally suited.

The goals of ad-network architecture for display advertising in online social media are largely the same as in display advertising in general: high effectiveness; rigorous privacy enforcement; support for cost-per-click and cost-per-thousand-impressions payment methods; automatic segment generation; scalability; and extensibility. To achieve these goals in social media, the ad network should function as an embedded, context aware, personalized, adaptive, and anticipatory part of the environment. In other words, in these environments, it must exhibit the properties of Ambient Intelligence (Aarts, 2004; Sadri, 2011).

The architecture proposed in this chapter, called *Amina*, pursues a semantic approach to higher response, organizing its processes to match the semantics of the targeted environment with that of an ad. The ad campaigns undergo two phases, called *bootstrap* and *performance*, in order to differentiate the pricing model, maximize the effectiveness of promising campaigns, and filter out early non-achieving campaigns. The key to the effectiveness are the architecture's segmentation processes, which construct contextual and behavioral models for the purposes of ad serving. The main observation behind these processes is that the same segment cannot generate both sufficient reach to bootstrap a campaign and required relevance for the effectiveness of the campaign. Instead, the campaigns are organized to: a) generate the reach and achieve minimal click goals through contextual targeting (bootstrap phase); then b) boost the performance of the campaign through automatic click prediction (performance phase).

By exploiting the semantics of the campaign processes, the architecture constrains data and mechanisms in order to support rigorous privacy guarantees. Its privacy features include: minimal data both in terms of content and duration; multiple levels of encryption and security; constraints on processes so that no property of user data is disclosed; enforcement of user and page privacy settings, the highest of which prevent collection of data; and a mode of operation that requires no user data. In addition to the rigorous privacy guarantees that the architecture supports as a baseline, an optional set of choices is given to all entities involved in order to enforce even stricter views on privacy.

We believe that the integration of display advertising into social media should always be approached with a good understanding of potential problems. The organization of the paper follows this approach. After focusing on the architectural core of the display ad network framework, we re-examine its premises

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/effective-privacy-first-display-advertising/228731

Related Content

The Ethics of AI and IoT in Healthcare: Navigating Cybersecurity Risks and Ensuring Data Protection

Sagar Sidana, Parul Chaudhary, Amrita Ticku, Nitasha Rathore, Anurag Sinha, Ashutosh Keshri, Biresh Kumar, Neetu Singh, Abhiraj Sinha and Neeraj Raj (2025). *Ethical Dimensions of AI Development* (pp. 347-368).

www.irma-international.org/chapter/the-ethics-of-ai-and-iot-in-healthcare/359651

The Role of the Profile and the Digital Identity on the Mobile Content

Ana Serrano Tellería (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1645-1664).

www.irma-international.org/chapter/the-role-of-the-profile-and-the-digital-identity-on-the-mobile-content/228801

Generative AI's Impact on the Hospitality Industry

Anam Afaq, Meenu Chaudhary, Loveleen Gaur and Rajender Kumar (2025). *Generative Artificial Intelligence and Ethics: Standards, Guidelines, and Best Practices* (pp. 243-266).

www.irma-international.org/chapter/generative-ais-impact-on-the-hospitality-industry/358934

Impact of Artificial Intelligence on Marketing and Consumer Decision-Making

Syed Aijaz Ahmad and Maroof Ahmad Mir (2025). *Generative Artificial Intelligence and Ethics: Standards, Guidelines, and Best Practices* (pp. 169-188).

www.irma-international.org/chapter/impact-of-artificial-intelligence-on-marketing-and-consumer-decision-making/358931

Cyber Security Patterns Students Behavior and Their Participation in Loyalty Programs

Witold Chmielarz and Oskar Szumski (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1247-1263).

www.irma-international.org/chapter/cyber-security-patterns-students-behavior-and-their-participation-in-loyalty-programs/228781