Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa|ON|K1N 6N5
cippic@uottawa.ca
www.cippic.ca

REPORT ON THE 2010 OPC CONSULTATIONS ON ONLINE TRACKING, PROFILING AND CLOUD COMPUTING

CIPPIC COMMENTS ON DRAFT REPORT

DECEMBER 20, 2010

Tamir Israel, Staff Lawyer

TABLE OF CONTENTS

INTRODUCTION

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) is pleased to present its comments on a draft recent report issued by the Office of the Privacy Commissioner of Canada regarding online tracking, profiling and targeting and cloud computing.[1] CIPPIC does not address all issues raised by this document, nor does it address each itemized feedback point. CIPPIC focuses its comments on consent, behavioural targeting, on the risks faced by online anonymity, and on identity management systems.

CIPPIC is interested in developing technical mechanisms that will enhance user control over online browsing and identity. In these comments, CIPPIC points to a number of concerns it deems must be addressed in order to maintain user confidence in online activities, generally, and attempts to demarcate where technical as opposed to regulatory solutions may be most appropriate.

I. IMPLICATIONS OF CONSENT

- *The OPC will continue to work with industry to develop the best approach to ensure that individuals are providing meaningful consent to legitimate business practices. This may be an area in which technology can prove helpful in addressing this problem. In that regard, we would welcome comments on how best to achieve this.*
- *The OPC welcomes additional views and comments regarding current and future online tracking and profiling practices (other than behavioural advertising) in Canada.*
- *The OPC challenges industry to find ways and means to help data expire and welcomes further discussions on this issue. PIPEDA is very clear that personal information should not be retained forever.*
- *The OPC would welcome further discussions with stakeholders on online identity management.*

A. Online Tracking: Behavioural Targeting

The Draft Report does a thorough job of setting out the parameters and risks associated with behavioural targeting. CIPPIC wishes to offer the following comments in order to refine the Report's discussion of these issues and their relation to consent. In CIPPIC's view, behavioural targeting and its accompanying online tracking, whether conducted by first or third parties, implies a business model that greatly challenges the balance between e-commerce and privacy that is intended to underpin fair information practices in the OECD guidelines and PIPEDA. It blurs the concept of 'legitimacy' by making data collection and marketing a primary and motivating element in various online business models.[2] It also puts in place strong organizational incentives that are diametrically opposed to those of their users – in fact, the user is no longer the customer in many behavioural targeting scenarios, but the *product*. In a free ad-supported service, revenues are dependent on getting more personal information and the true customers are the advertisers.[3]

This blurring of what is legitimate and reasonable is accompanied by a technical complexity and obscurity that few customers can hope to understand. The pervasiveness and ubiquity of online tracking, for example, is opaque to web surfers and the techniques used to accomplish it are "nearly impossible to detect" and prevent.[4] It is also very important to note that, even more opaque and impossible for a surfer to quantify, is the aggregation and analysis to which

her data will be subjected once collected and the assumptions and decisions that will result.[5] Perhaps most troubling, it is impossible for a netizen to know who is tracking them when or for what purpose, as the tracking itself is invisible. The Draft Report does an effective job of pointing out the harm that may result from decision-making based on inaccurate information accrued through tracking, as well as the fact that the risks of aggregation extend to identity construction and autonomy.[6] As noted in a recent FTC report on the issue of online tracking, "for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'"[7]

Part of the issue, in CIPPIC's view, is the blurring of legitimacy that emerges from online tracking. In spite of strong and clear statements to the contrary by international bodies to date,[8] many organizations operate under the implication that customers expect and desire tailored advertising today and, in fact, view it as a benefit.[9] Some companies operate under the assumption that customers wish to establish 'social' relationships with brands and companies.[10] This, in turn, justifies any online tracking that occurs in order to provide a more tailored and social marketing experience. It is important, in CIPPIC's view, to clarify this issue. Few customers view any advertising as a 'benefit', but rather something one must put up with. Indeed, the government is in the process of passing legislation that will impose hefty regulatory penalties for communication of unsolicited commercial messages.[11]

Research indicates that while some (32% [note: 55% for those aged 18-24]) may prefer that the advertisements imposed on them at websites be tailored as opposed to non-specific, this group shrinks dramatically when the tailoring results from first party tracking (to 24% [33% 18-24]) and even more so where third party tracking is required for that tailoring (13% [14% 18-24]).[12] Further, a recent US-based Gallup pole suggests a sizeable proportion of customers would be comfortable opting in to specific, known, and trusted advertising networks, but are concerned with the current unrestrained, impossible to monitor free for all situation, whereby any advertising network can track anyone, unbeknownst to them, and for whatever purpose.[13] In addition, there appears to be little customer understanding of the value exchange that occurs with ad-supported services.[14] While customers may benefit from access to some of the services that are funded by online tracking,[15] this does not, in CIPPIC's view, legitimize tracking in the absence of clear customer consent. Indeed, CIPPIC views the scope of some such tied selling proposals with great concern.[16] The current free for all, where anyone can track anyone else for whatever purpose is, in CIPPIC's view, unreasonable. While there may be circumstances where consentual tracking is legitimate and acceptable, in others it is not. In CIPPIC's view, it is important to start to examine the parameters of that reasonableness.

Users must be provided with a simple, effective mechanism to monitor and, if they so choose, prevent online tracking.[17] In CIPPIC's view, any such mechanism should be browser based. A user-agent (browser)-based tracking control has the greatest opportunity of effectively ensuring that user preferences are respected. It additionally will be more intuitive, merging the tracking control mechanism squarely within the medium for browsing. Finally, it is fitting and appropriate to locate tracking controls with the browser. Indeed, when cookies were first

proposed as a mechanism for maintaining state across multiple visits or webpage hits, browsers were intended to adopt certain mechanisms in order to prevent their use for tracking purposes. These mechanisms included the blocking of third-party cookies by default,[18] but the majority of browsers have never implemented this imperative.[19]

In this respect, there are a number of promising user-agent-based mechanisms for enhancing user control over online tracking.[20] The FTC, for example, has called for user-agent browsers to develop and implement a simple mechanism for consumers to signal a 'Do Not Track' intention to would-be behavioural targeters.[21] This approach bears similarities to a 'do not crawl' robot script currently used by website developers to signal to search engine robots what information should and should not be scanned for searchability.[22] It would adopt a universally recognized signal, perhaps akin to a persistent cookie, that notifies all advertising networks not to track. It would succeed in dong so without relying on a unique identifier to indicate opt-out intent. [23]

In CIPPIC's view, any such 'Do Not Track' mechanism must be adopted to provide granularity, so that users who wish to do so may opt in to specific advertising networks while continuing to block less desirable networks.[24] Any such mechanism must additionally be technically neutral so as to transcend organizational attempts to subvert user intentions based on technicalities such as whether tracking is accomplished via a flash cookie or other object instead of by HTTP cookie.[25] In contrast to many existing industry opt-out mechanisms, it must also prevent *collection* of user browsing and not merely replace targeted advertisements with non-targeted ones.[26] Such a mechanism, to the extent that it relies on industry compliance, must be accompanied by strong penalties for non-compliance given the difficulty in overseeing organizational activities.[27]

CIPPIC envisions a regulatory role in bringing about solutions of this nature. In CIPPIC's view, by enabling storage of and access to tracking objects such as cookies on user computers, browsers are facilitating online tracking. Speaking more generally, it is CIPPIC's position that, as user activities are intermediated to greater extents through centralized points of access control such as browsers, mobile phones, or other services such as those offered by social networking sites, an expanded role for such intermediaries in taking positive steps to protect user privacy will be essential. This is becoming increasingly imperative with the addition of geolocational tracking capacity to the already broad tracking capabilities facilitated by these types of services, including browsers.[28]

B. 'Other Purposes' & Privacy Concerns

The draft discussion document requested input on online tracking that is not advertising based. In CIPPIC's view this is an important developing area of tracking that bears serious examination. CIPPIC is particularly concerned with online tracking presented as 'primary' or 'necessary', but which can only loosely be referred to as such, as well as tracking facilitated by non-commercial user-generated activity and by disclosures 'authorized' by friends of individuals.

(i) Tracking 'necessary' to improve your service

The type of tracking that CIPPIC is concerned with under this category is primarily data that is being collected and used for the purpose of 'product/service improvement'. Users are typically notified of the purpose for such collection, retention or use in a very imprecise manner, of which the following are indicative:

> Facebook:
> **To manage the service.** We use the information we collect to provide our services and features to you, to measure and improve those services and features, and to provide you with customer support.[29]
>
> Google Search:
> **User communications** – When you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services.[30]
>
> Amazon:
> The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.ca. Here are the types of information we gather.[31]

Sometimes greater details on some specific practices are provided, at other times they are not, even though this type of notice is used, apparently, to justify a fairly broad range of activity. Sites such as Amazon and Yelp!, for example, use it to predict product preferences so as to present users viewing an item with targeted advertisement suggestions of similar products they may wish to purchase. Google may be using (and retaining) such data (likely in anonymized format) to perfect its various algorithms.[32] Facebook uses such data to 'map' the nature of social connections between individuals. It does this to 'recommend' new friends to increase user engagement with the site.[33]

It is unclear what else may fall within this potentially broad category of 'improving our services to you.' For example, Facebook appears at one point to have been experimenting with a tool capable of predicting who will 'enter a relationship' with whom based on an analysis of user interactions.[34] Additionally, Google appeared to view its collection of WiFi hotspot identifiers for the purpose of improving its location-based services as 'legitimate'.[35] As noted above, many online advertising organizations such as Facebook justify the collection and retention of browsing activities on third party websites in order to help improve their advertising services as well:

- We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see.
- We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.[36]

In addition, the 'operational' imperatives of Facebook Open Graph API tools such as the 'Like' button facilitate an unprecedented and effectively unavoidable level of user tracking across several third-party services.[37] Basically, Facebook is notified whenever a user visits a website with Open Graph API functionality (such as the 'Like' button) whether the user interacts with any Facebook features of the site or not and, apparently, regardless of whether the user is logged in to Facebook at the time or not.[38] The 'Like' button operates, in this respect, much like a standard web bug.[39] While Facebook *currently* does not use such data for advertising purposes it does retain it for 90 days and, in anonymized format (for the purpose of improving its products) seemingly indefinitely.[40] Facebook notes that this is "consistent with standard industry practice".[41]

Customers have legitimate concerns, in CIPPIC's view, with respect to the fact of tracking, irregardless of whether this information is inevitably used for an advertisement or not.[42] In addition, given the well document ease of de-anonymization, there are valid questions with respect to whether this is a legitimate means of data retention.[43] CIPPIC notes that the retained information does, for Facebook, serve a commercial purpose in that it allows the service to advertise the prevalence of its reach to its advertising constituents.

At the outset, it is CIPPIC's view that there are likely legitimate and non-legitimate uses that may be encompassed by the 'product/service improvement' rubric. Our concern stems from the breadth of these types of provisions and the lack of transparency with respect to what type of tracking/data retention is justified by such purposes. This is particularly problematic in light of increasing ambiguities with respect to the prospects of de-anonymization.[44]

(ii) Privacy Invasion by Non-Protected Purposes

CIPPIC is additionally concerned by tracking that is motivated by purposes currently exempted from PIPEDA altogether. Professor Scassa, for example, highlights the potential for much user-generated fact-based information to fall within the journalistic purposes exemption of PIPEDA.[45] Professor Scassa recommends amendments to PIPEDA's journalistic purposes exception to narrow its scope so as to expressly incorporate a 'reasonableness' criteria that balances the level of intrusiveness of the data being disclosed and the public importance of the information in question.[46] CIPPIC notes that in other jurisdictions, Courts have applied a similar balancing test to journalistic organizations within the context of the common law tort of invasion or privacy.[47]

CIPPIC is similarly concerned with the lack of protection under PIPEDA for privacy invasions that may now, in an increasingly inter-networked world, occur outside the scope of any commercial activity but by pure individual effort.[48] While some or much such activity may fall outside the scope of federal data protection legislation, there should at the least be scope for the exploration of solutions to the privacy issues that are raised by the online capacity of individuals to injure the privacy of their counterparts outside the context of commercial activity.

(iii) Collection authorized by third parties

CIPPIC is greatly concerned with the potential scope of online tracking and privacy invasion which may result where consent is sought, not directly from the individual herself, but by proxy

from a 'friend' or other individual. This is particularly concerning in situations where information provided in this manner becomes or is associated with metadata, where it is placed on some readily accessible application platform, and/or where the consent encompasses secondary purposes including marketing.

It is important to clarify that in such circumstances, as noted by this office, it is imperative to gain the informed and express consent of the individual directly.[49] Where this is impossible (and it should be *only* where this is impossible), then reasonableness criteria should be applied. It may, for example, be reasonable to imply consent to some disclosures but not others. But there are certainly circumstances where this is not the case. CIPPIC is particularly concerned over situations where potentially sensitive information such as location is indelibly recorded in searchable format or transformed into metadata made available to hosts of developers.[50]

C. Privacy by Effort

The draft notes comments to the effect that many online services are designed around the 'public by default, privacy by effort' architectural design principle.[51] The Draft Report does a good job of highlighting some of the concerns for managing one's identity online, and CIPPIC wishes to elaborate a little more on this concept.

The Draft Report speaks of consent and highlights many of the difficulties inherent in explaining to customers precisely what they are consenting to in a meaningful way, particularly with respect to online tracking and behavioural analytics.[52] It is CIPPIC's position that the form of consent is a critical element in the determination of whether consent is 'meaningful'.[53] CIPPIC notes that industry opposition against a rule that would require users to take active steps before consent can be inferred focuses on the impact on user experience.[54] CIPPIC would first of all like to note that requiring users to opt out of features, services, or settings a user considers insufficiently protective of privacy is equally if not more so disruptive of user experience – more so because 'opt out' mechanisms will often be more difficult to find and understand than 'opt-in' mechanisms.[55]

CIPPIC believes it is important to note that the difficulties inherent in attempts to acquire meaningful consent will often be multiplied, in its view, in situations where a new service or feature is being superimposed on a pre-existing one. In such situations, users are often not given time to examine new features or their implications and will often take organizational 'recommendations' or 'defaults' as given.[56] This is especially the case where the changes are transformative in that they change the nature and character of the existing service in a manner that is privacy-salient (a sudden 'complete change in policy'). One example of this, in CIPPIC's view, is Facebook, which recently transitioned many of its millions of customers to a more 'open' business model where much sensitive information was made publicly available by default.[57] Another example is Apple's recent introduction of geolocational-based advertising on its iPhone platform.[58] Yet another is Google's introduction of its Buzz social services into Gmail.[59] CIPPIC notes that central to each of these three incidents was the misuse of opt-out consent mechanisms and, of the three, only one led to retroactive steps to address the privacy concerns that were raised.

The Draft Report notes the amount of effort that is required of customers to discover, investigate, understand, and then attempt to address privacy concerns raised by online behavioural tracking – it asks, "[i]s this reasonable to expect of the average user?"[60] CIPPIC believes that this question is integrally linked to the issue of behavioural targeting, as it will often be the means by which information of users is put 'out there', to borrow a term from the Draft Report.[61] Generally speaking, but specifically with respect to a platform with a captive audience of users, it should not fall to the customer to run a gauntlet each time a new service is introduced simply to maintain their privacy. As noted recently by the FTC:

> …choices buried within long privacy policies and pre-checked boxes are not effective means of obtaining meaningful, informed consent. Further, the time and effort required for consumers to understand and exercise their options may be more relevant to the issue of informed consent than whether the choice is technically opt-in or opt out.[62]

Additionally, it is important to note that with respect to online tracking, customers express a strong preference that organizations ask before tracking using 'opt-in' mechanisms.[63]

Further, CIPPIC views 'take it or leave it' choices problematic and particularly so in an online environment where decisions are often made quickly and vast amounts of data may be exchanged with little time for introspection.[64] There is strong support for the proposition that, when presented with quick, all or nothing, authentication methods in this manner, users will provide the requesting organization with far more information than necessary to achieve its purpose, simply for ease of access.[65] This will be particularly problematic where the disclosure is a condition of using the authentication mechanism. At the same time, websites who are aware that there is a readily accessible treasure trove of information for the asking are far more likely to require more information than is needed to provide their service.[66]

In sum, CIPPIC believes that 'transparency' is necessary, but by no means sufficient in an online environment. Indeed, such an environment presents organizations with various opportunities to create creative consent mechanisms that ensure users are, in fact, agreeing to online practices. Particularly on a platform such as a social networking site where changes are constant and repeated, it is neither fair nor reasonable to expect users who wish to maintain even a constant level of privacy to audit their user accounts on a weekly basis or each time a new 'feature' is introduced to figure out how to opt-out of it.[67] It may be worthwhile, in this respect, to re-explore what 'express' means in the context of an online environment.[68]

II. CLOUD COMPUTING: SECURITY ON THE CLOUD?

CIPPIC will limit its comments on cloud computing to one issue of great concern to it that it sees as antithetical to customer confidence in the shift towards cloud computing. Specifically, CIPPIC is concerned with the expansive investigative role online intermediaries are being asked to undertake in a number of contexts to fulfill public policy objectives. CIPPIC is concerned by the lack of safeguards in place preventing disclosures by private organizations in aid of civil and public law enforcement.

This lack of safeguards will be detailed in brief below, but the concern from a civil society perspective is that there are increasingly fewer protections in place preventing private organizations from mobilizing the personal information of their customers in investigations against them. These concerns, already significant, are dramatically expanded in a cloud computing based world where increasing amounts of information are entrusted to third party entities and therefore subject to disclosure upon request by a civil plaintiff or a government agent.

A. Civil Liability

With the rise of social networking and other forms of computing, civil litigants are beginning to discover the treasure trove of personal information that they may now acquire through discovery processes and use against their opponents in Court. To date, most third party disclosure suits have involved the identification of anonymous defendants, typically in the context of alleged intellectual property infringement or alleged defamation.[69] Some have involved tort suits have asked intermediaries to disclose metadata regarding online activity of a party.[70] In still other suits, defendants have sought detailed online information directly from parties, demonstrating the extent to which such information is viewed as useful and relevant in civil suits.[71]

While courts are developing safeguards that govern the conditions under which such information will be disclosed *within* discovery processes,[72] it is not clear that PIPEDA prevents the disclosure of this type of information, and especially of identification information, in the pre-discovery stages of the process as long as customers are provided with sufficient notice that their information may be disclosed by the intermediary to assist a civil litigant pursue a lawsuit. Whereas a potential litigant may decide on her own whether to challenge a disclosure request for information in her possession, she, of course, cannot where the information is held by a third party and where she is not aware of the request.

CIPPIC is especially concerned with tabled legislative changes that will clarify and legitimize disclosures of this nature in the context of potential civil wrongs.[73] The immense amounts of personal information that will be reposited with online intermediaries are, in CIPPIC's view, a direct product of e-commerce and the added vulnerability Canadians are subjected to by depositing their information in such contexts directly impacts on consumer confidence in cloud computing, and e-commerce generally.[74]

B. Criminal Investigations

Far more serious in the context of cloud computing is, in CIPPIC's view, the impact that shifting to the cloud may have on the expectations of privacy Canadians may be permitted to reasonably hold. A string of cases have held that the reasonableness of any expectations of privacy users may have in data disclosed to third party intermediaries is largely, if not wholly, dependent on whether the organization has notified the individual through its terms of use that it may, at its discretion, disclose information to assist in a law enforcement investigation.[75]

Since Parliament intends to broaden PIPEDA exceptions to disclosures of this type in serious ways,[76] and even add mandatory disclosure mechanisms,[77] there are serious and valid concerns that much Canadian information entrusted to cloud services will be at the beck and call of government agents.[78] Given the increasing scope of information to be entrusted to the cloud as well as growing analytical capacities to process such information, its potential impact on civil liberties is significant.

At this stage, it appears that the policies adopted by service providers will have significant impact on what privacy Canadians can reasonably expect with respect to information entrusted to those service providers. Most service providers include broadly phrased statements reserving to themselves the right to disclose information to law enforcement upon request. The following is indicative:

> …you agree that Your Service Provider reserves the right to monitor the Service electronically from time to time and *to disclose any information necessary to satisfy any… governmental request* or *as necessary … to protect… others.* [79]

As such broad notices seem sufficient to impact on user expectations of privacy,[80] it is imperative, in CIPPIC's view, that service providers commit to limiting themselves contractually to either refrain from disclosing information to law enforcement in permissive circumstances or, at the very least, to doing so in extremely limited circumstances.

III. IMPORTANCE OF ONLINE ANONYMITY & THE PUSH TOWARDS IDENTIFICATION

- *The OPC would welcome further discussions with stakeholders on online identity management.*
- *The OPC challenges industry to find ways and means to help data expire and welcomes further discussions on this issue. PIPEDA is very clear that personal information should not be retained forever.*

> Market forces encourage architectures of identity to facilitate online commerce…If anything is certain, it is that an architecture of identity will develop on the Net—and thereby fundamentally transform its regulability.[81]

> A Democracy that purports to value individual autonomy and privacy must place limits on when and how a person is required to identify him- or herself and, how much information is required to participate in society. At the same time, identity policy must address the legitimate needs of governments and the private sector for information about an individual that enables them to conduct business with the individual, provide services to or administer programs for the individual

> ….our society possesses increasingly advanced tools that allow the type of extensive surveillance that is characteristic of authoritarian societies. We may have the good fortune to live under governments that in general respect rights, but no Canadian, and no citizen of any democratic country, should take it for granted that their governments will always reject authoritarian methods.[82]

In an online world where much activity must, given the nature of the medium, occur in a semi-public environment, anonymity is an essential key to any realization of privacy. The ability to

act anonymously may be the only means to act privately in many online contexts. Further, the use of a pseudonym may, in some scenarios, have important legal salience in analyzing expectations of privacy.

Yet the concept of online anonymity is under increasing pressure from a "proliferation of various security measures in the public and private sectors designed to undermine the 'ID-free' protocols of the original network."[83] Online anonymity is integral for a number of reasons, and, particularly on the online sphere, is integrally tied to rights of free expression and privacy.

CIPPIC believes the consultation document may be enhanced by an acknowledgment of the importance of online anonymity as well as of the pressures being brought to bear on an individual's ability to act anonymously online. In support of this claim, we offer a number of examples below that we hope are indicative of the increasing difficulty confronting an individual wishing to retain her online anonymity.

A. Obligations to Self-Identify

A number of online services are beginning to require users to provide and, at times, even to display real life identities in all dealings, meaning that any activities displayed by the site in question will, in theory, be associable with a real life identity. Where there is no legitimate need for such requirements, this is concerning. There are several examples of this.

(i) Online News Publications

A recent backlash against online anonymity has, perhaps somewhat ironically, manifested in the online news industry, with many online publication sites putting in place measures to discourage anonymous commenting on articles.[84] The tipping point for this phenomenon appears to have been one online publication's decision to identify to the world an online commentor whose identity it had discovered and deemed newsworthy. The Cleveland 'Plain Dealer' decided to determine the identity of a frequent commentor on its posts, 'Lawmiss', after the anonymous individual had made abusive comments, disparaging a relative of a Plain Dealer reporter. Lawmiss was identified when a Plain Dealer employee discovered (it is not clear how, but a simple Google search would likely have done the trick) that the email used to open Lawmiss' Plain Dealer account was associated with the AOL account of a local County Judge.[85] This identity was deemed newsworthy, and the paper revealed it in a subsequent news article.[86] This act of identification re-sparked a debate in the news industry on whether anonymous comments should or should not be allowed, leading several publications to adopt various measures to prevent anonymity.

This is done by a variety of methods. Some use 'soft' methods by providing subtle and not-so-subtle incentives for using persistent or real life identifiers.[87] Such incentives include internal systems that display authenticated commentors more prominently, for example. More concerning in this particular context are harder measures against anonymity, such as new obligations to register with real-life identity before participating in online discourses (users may still comment pseudonymously, but the publication requires prior authentication, typically in the form of a confirmed email address).[88] Most troubling are methods similar to those adopted

by the Wall Street Journal, which has now taken away the capacity to comment anonymously altogether – users must register and may only comment using their real names.[89]

The impetus for what Arianna Huffington of the Huffington Post refers to as a "trend…away from anonymity", is a belief that anonymity is the source of the 'offensive commentary' that perhaps too frequently peppers the comments strings on online newspaper articles.[90]

The axiom that "providing identity says little about the trustworthiness of an individual" is, in CIPPIC's view, as applicable to online decency as it is to security concerns[91] – the perceived degradation of online discourse cannot be so easily pinned on anonymity.[92] Regardless of the legitimacy of such attempts at forced identification, our concerns with the impact such site requirements may have on privacy and online anonymity stand. While, at this time, verification of online identities in venues of this nature is not stringent – all that is required is an email address – the current trend is troubling and the potential for online publications of this nature to step up identity verification is, in CIPPIC's view, significant.[93] Individuals should be permitted to act anonymously in such situations, particularly where the benefits of stringent identification requirements are not clear.[94]

(ii) Email Registration

Another example of a troubling trend against online anonymity is the recent emergence of stringent verification processes as a mandatory element of once innocuous registration processes. Google, for example, now makes phone-number based verification a mandatory component of its Gmail registration process.[95] Google explains this new identification requirement as such:

> **Why am I being asked to provide a mobile number?**
> In an effort to protect our users from abuse, we sometimes ask users to verify their identity before they're able to create or sign into accounts. We take spam and abuse very seriously, so there are numerous things we do to block spammers and their messages. Sending verification codes to phones is one way to verify that real people, not robots, are creating and signing into Google Accounts.[96]

Users are informed during the signup process that the number will be retained, and used for the following purposes:

> Account verification helps with:
> - Preventing spam: we try to verify that real people, not robots, are creating accounts.
> - Recovering account access: we will use your information to verify your identity if you ever lose access to your account.
> - Communication: we will use your information to notify you of important changes to your account (for example, password changes from a new location).[97]

This makes it clear that the real-life phone number is not simply a one-off verification mechanism to ensure the registrant is a 'real person' at point of registration. Rather, it will act as a continual link between the individual's gmail account and her real-life identity. Provision of

a phone number is mandatory. Users who do not have one and wish to open an email account are advised to "ask a friend to use his or her number".[98]

While email sites such as Gmail have always nominally required users to enter a real name and other similar verification information, it is common practice, at least, for individuals to have pseudonymous email addresses that are not readily traceable back to a unique identity.[99] Indeed, the email address is in many sense the building block of anonymous online activity as it permits for a sometimes necessary channel of ongoing communications with a website or service that need not be linked to any real life identity. While this required real-life link is motivated by legitimate purposes (to prevent spam, fake accounts used for illegitimate reasons), and while Google continues to provide users with the capacity to create multiple accounts, CIPPIC views this as part of a general 'trend' towards eroded online anonymity.

(iii) Social Networking Sites

Social networking sites such as Facebook require users to provide a real name at registration. Users are then prevented from carrying out any Facebook activity under a pseudonym of any kind. Significantly, where a user registers with a third-party website such as the Huffington post using Facebook's registration process, the website is always provided the user's real name.[100] Some websites then offer users the option of adopting a different user name for their on-site activities.[101] It is a violation of Facebook's terms of use to provide it with a false name and the site has been known to proactively monitor accounts for fake looking names and delete those that it does not deem 'real'.[102] Indeed, before Facebook permits its users to change their names, it requires them to ask it for prior approval of the newly chosen name and limits the number of name changes allowed per account.[103]

Facebook has additionally begun employing both soft and hard measures to link user accounts to real-life confirmable identifiers such as mobile phone numbers. Facebook now employs, for example, a similar phone number-based verification process before permitting a user to customize her profile URL.[104]

In addition, it has taken to prompting users to provide it with their mobile phone numbers in order to "update your security".[105] Users are told that, without providing a verified mobile number, they cannot achieve a "'High' Account Control level".[106]

While CIPPIC recognizes Facebook's interest in encouraging users to use 'real' identities,[107] there are many legitimate reasons for a user to wish to act anonymously on Facebook[108] or on other Facebook integrated sites across the Internet.[109] Similarly, with respect to security-motivated rationales for linking Facebook accounts to real-life identifiers such as phone numbers, CIPPIC views that the means of achieving such objectives should be proportional to their purported benefits.

B. Cross-Platform Identities

Clark, *et. al.* describe anonymity as comprised of two necessary elements:

> P1: an anonymous action is not linkable to the identity of the actor, and P2: two anonymous actions performed by the same actor are not linkable to each other.[110]

Neither, in and of itself, is sufficient, and limitations on cross-platform identities threaten the second (P2) element of anonymity identified by Clark. The concern is the increasing use of a single persistent login across multi-platform services provided by the same service provider. The concern emerges from the fact that multi-tab browsers have become the norm in web browsing today. Given this system, many users will stay logged in to one service (email, a social networking site, etc.) in one tab while browsing other sites. As access to the 'logged in' status and unique identifier associated with the email or SNS account in question is controlled by cookies, the user's browser will permit the Email/SNS service provider to access this information from any of the other tabs a user may open.[111]

So, for example, Alice signs in to her Gmail account in one tab of her browser and continues browsing, leaving Gmail open so she may continue to monitor her email. Her logged in status and a unique identifier for her Gmail profile will be controlled by a cookie, which her browser will permit Google to access from its myriad services. Later, she is watching YouTube videos and wishes to enter a comment. She is required to log in to her YouTube account, and (assuming it is distinct from her Gmail account) by doing so, will automatically be logged out of her Gmail account. This imposes a 'soft' cost on users who wish to maintain greater anonymity using diverse identities across Google's myriad services.

Other models of cross-platform identification are more problematic. If Alice is logged in to her MS Hotmail account, for example, and attempts to log in to a second MSN service such as Xbox or Bing in another tab, MS will automatically use her Hotmail account if she clicks 'sign in'.[112] Before MS will permit her to sign in with a distinct account, Alice must go to the Hotmail tab and physically log out. While both Microsoft and Google currently permit Alice to adopt different usernames across these different platforms for any visible online activity she intends to undertake, it is often possible for a third party to read past such pseudonyms, as Justice Saffold ('Lawmiss') discovered.[113]

Another issue raised by cross-platform identities is with respect to Facebook's third party identification method. As mentioned above, any website can use Facebook's Graph API to register users for its internal services instead of requiring users to register independently. Once the two accounts are 'linked', login across the two is mutually linked as well. This means, for example, that if Alice registers for the Huffington Post using her Facebook account, whenever she visits the Post while logged in to Facebook, she will automatically be logged in to her Huffington Post account as well. Further, if she attempts to log out of her Huffington Post account she will similarly be logged out of her Facebook account. Alice is not given the option to remain logged in to one, and anonymous on the other.[114]

The issue is that it becomes very difficult for individuals to use different identities across different services at the same time. The threat to anonymity this may pose increases, of course, with the diversity of services offered by a particular platform.[115]

C. Increasing Risk of De-Anonymization

The point has been made at various points above as it touches on online privacy in a number of contexts, but it deserves reiteration here.[116] The ability to de-anonymize online data increases in direct proportion to the amount of data publicly available and the constantly evolving algorithms available to analyze it. This risk further undermines the ability of users to act anonymously online, as well as overall trust and confidence in online environments.[117]

IV. ONLINE IDENTITY MANAGEMENT

- *The OPC would welcome further discussions with stakeholders on online identity management.*
- *The OPC will continue to focus our outreach activities on individuals to help them better protect themselves online. This will include exploring how best to help individuals focus on privacy explanations that are provided to them. The OPC welcomes any comments on how best to achieve this.*

Identity management is, of course, intricately tied to online anonymity, privacy, and other civil society concerns noted above. The failure of centralized government-based identification systems in the off-line 'brick and mortar' world[118] is indicative of the general resistance any online identity integration system may face if it is not carried out in a manner that respects user privacy. A properly implemented identity management (IdM) system can be greatly enhancing of privacy, solving many current issues in online browsing, anonymity, and privacy. On the other hand, an improperly designed and implemented IdM solution will merely exacerbate existing online privacy problems while introducing new ones.[119] CIPPIC is, of course, greatly supportive of the former, while the latter is not likely to gain user confidence and trust.

The potential benefits of a properly implemented IdM system include enhanced security, as passwords are aggregated in one location and information flows are, perhaps, minimized expressly to what is necessary.[120] Additionally, using third party authentication and establishing reliable online identity may reduce the chance of fraud and identity theft. But IdM systems are inherently riddled with potential contradictions that, if not properly navigated, would undermine any benefits they may have.[121] As noted by some, any effective IdM system must be accompanied by strong regulatory protections.[122] As such systems rely heavily on user consent, strong regulatory assurances that consent will be meaningful are an essential precursor to any implementation of an IdM system.[123]

Briefly, an IdM system is one that facilitates the claiming and authentication, and authorization of online identity.[124] In this context, the term 'identity' refers simply "to a claim or set of claims about the user".[125] A 'federated' IdM system allows service providers a user has selected to rely on trusted third parties to authenticate services on the user's behalf.[126] There are four essential entities in a federated IdM system: [127]

- **User**: The end user who is attempting to interact with an online service
- **User Agent**: The user will always be conducting this interaction through a user agent – typically a browser (including mobile browsers).
- **Service Provider/Relying Party (SP/RP)**: The web-based application or service that is essentially outsourcing a registration or authentication process and is relying on the IdM system to accomplish this task effectively.
- **Identity Provider (IdP)**: A second web-based entity that conducts the authentication/registration process and may additionally store further User information that may be shared in various ways with different RPs. Some federated IdM systems allow for multiple IdPs within a 'circle of trust'.[128]

There are three main IdM mechanisms that are typically recognized in the literature, each of which is useful for different contexts:

- OpenID, a scalable, open source that is omni-directional.[129]
- SAML (Security Assertion Markup Language), which underlies Liberty Alliance protocols and implementations and provides perhaps the most comprehensive and diverse IdM metasystem.[130]
- Cardspace, Microsoft's implementation of its InfoCard protocols. A operating-system based IdM system with an intuitive user interface.[131]

Some add SNS-based registration processes to this list.[132]

The Public Voice has outlined civil society concerns with IdM in a backgrounder and set out a number of design principles that any successful effort at an IdM system must commit to.[133] CIPPIC adopts these in the following manner:

- **Minimal Disclosure**: systems must be designed to disclose as little as is absolutely necessary to provide the service or transaction in question. As noted in the Civil Society Backgrounder, "full anonymity must be the default option, and single information bits are then added consciously and sparingly."[134] CIPPIC notes that this principle becomes very difficult to quantify where secondary and primary purposes blur as well as where services incorporate 'social' elements that may justify varying ranged of information disclosure.[135]
- **Non-Linkability**: Any IdM system must be capable of accommodating multiple unique identifiers across different services to prevent unintended aggregation/tracking across several service providers,[136] to prevent unauthorized identification,[137] and to facilitate anonymous activity across different services.[138] Non-Linkability is the IdM mechanism that facilitates 'contextual integrity' across diverse online activities. It is, from a privacy perspective, the core benefit that federated IdM can offer. Without non-linkability, an IdM system may provide "a remarkably invasive look at an individual's life."[139]
- **Non-Traceability:** The IdP is placed in a unique position to track user activity and aggregate user information at potentially unprecedented rates, particularly where one single IdP is used across multiple services, types of information, contexts, etc.[140]

- **User-Centric:** Any IdM system must place the user in control of all information flows and must allow the user to see what information is being accessed by which Service Provider.[141] The form of consent and the interface must be one that facilitates meaningful consent.[142] Further, secondary purposes such as marketing, profiling, etc., must, under such circumstances, be require express and distinct user opt-in. Similarly, IdPs and SPs must be prevented from making arbitrary and retroactive changes that impact on their users in significant ways.[143]
- **Information Held by Other Users:** a successful IdM system must be designed in a manner that will recognize that personal information held by two users raises privacy issues for both and belongs to both. Services allowing users to publish information about others must gain consent of both parties.[144] This is particularly imperative given an apparent move towards 'relationship-based' methods of establishing trust in IdM systems.[145]

As noted, CIPPIC believes a properly implemented IdM system can greatly enhance online user privacy and anonymity. CIPPIC points to the following issues as potential barriers that may prevent user buy-in/confidence in an IdM system:

- **Consistent interface**: This is a problem with some web-based IdM systems. Users are required to leave the webpage they are on in order to 'sign in' to another service elsewhere.[146] This consistency improves usability and also reduces phishing risks.[147] In CIPPIC's view, a user-agent/browser-based solution is ideal for maintaining consistency of user experience. While some may argue that this conflicts with a trend towards the cloud, this need not be the case, as many have noted that a browser-based, well established IdM mechanism can form a strong basis for user trust in cloud-based services.[148] A user-agent-based interface is also integral to any truly user-centric solution as it will place the user in
- **Consent to Secondary Purposes/Aggregation Cannot be Assumed:** IdPs and SPs cannot imply user agreement to secondary purposes such as marketing or to aggregation/analysis of personal information, even for primary purposes other than those strictly necessary for system operations.[149] This includes, in CIPPIC's view, use and retention of personal information for internal analysis/improvement of services, even if in anonymized form, where it can be readily de-anonymized.
- **Avoid Oversimplification of interface:** Consistency in interface must not be synonymous with simplicity of interface. An oversimplified interface, where users are not compelled to decide which specific items of information to provide in each case is likely to lead to over-sharing of information.[150] IdM systems rely on user critical consent as a key mechanism in ensuring its objective of minimal disclosure.[151] Given this and the potential sensitivity and scope of the information being transmitted and the ease of disclosure from the user perspective, robust consent requirements is an essential prerequisite to any effective IdM system.
- **No Substantive Unilateral Changes:** Users must have strong and binding assurances that there will not "[a]ll of sudden [be] a complete change of policy"[152] in IdP or IdM

processes that will leave a majority of users exposed in significant ways. Any unilateral changes to IdM or IdP business models should be taken with the greatest of care and only, again, with robust consent.[153]

- **User Ability to Assess SP Policies:** Given the ease and rapidity facilitated by IdM systems, it is important that users are provided with more robust mechanisms for assessing service provider or IdP policies and for opting out of secondary purposes. To this effect, some have stated it is the obligation of the IdM system to inform users whenever an IdP is selected that has the capacity to track online behaviour.[154] Further, a truly user-centric IdM system should provide users with the ability to set contractual terms for themselves, within reason. The development of standardized privacy agreements and simple representative icons can provide users with a range of options in determining how their relationship with a given SP or IdP will be governed with respect to their personal information.[155]
- **Intermediary Investigation Assistance:** While all entities in the IdM chain must and can be expected to comply with information requests mandated by a court order, warrant, or other lawful imperative, IdPs, at the least, should commit in terms of use documents to non-disclosure of any information unless mandated to do so by law. Lacking such commitment, users will be surrendering more information for potential use against themselves in future criminal or civil investigations.
- **Anonymity:** An effective IdM system must also permit users to interact with Service Providers pseudonymously where the SP has adopted a policy mandating real-life identity, if users choose to do so. This may hinder the reliability of online credentials in some circumstances, but is necessary in light of the recent 'trend' away from anonymity.[156] In addition, an IdM system should permit multiple concurrent sign-ons, as does OpenID. So, for example, a user-agent-based (browser or otherwise) solution should permit multiple concurrent user-agents in addition to multiple concurrent 'identity cards/profiles' within a specific user-agent. This is to avoid a website from mandating a 'real' identity where the legitimacy of that request is questionable. Additionally, IdMs should minimize the amount of real-life mandatory information users must provide. If not required for any services, identifiers such as SIN or a phone number should not be mandatory for the operation of an IdM metasystem.
- **Online Tracking/Behavioural Targeting**: If a user-agent-based IdM system is to operate as a mechanism for consent to online tracking/behavioural targeting, the controls for such tracking/targeting must be built into specific identities (so that users may operate under non-tracking identity/profiles, or opt select tracking companies into one specific identity/profile and only that profile).

CIPPIC shares the OPC's interest in IdM systems and believes that, properly implemented, such systems may be an effective mechanism for increasing online privacy and anonymity. To do so, however, strong technical, regulatory and other mechanisms must be in place to ensure the concerns noted above are addressed.

[1] Office of the Privacy Commissioner of Canada, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing*, October 25, 2010, DRAFT FOR COMMENT, ["Draft Report"].

[2] PIPEDA Case Summary #2009-008, <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>, at paras. 130-131. S. Barocas & H. Nissenbaum, "On Notice: The Trouble with Notice and Consent", *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009, <http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf> point out at p. 2 that aside from the online tracking that behavioural targeting relies upon to populate its user profiles, such advertising models are dependent on tracking user activity to measure the success of cost-per-click and cost-per-action pricing mechanisms and to prevent click fraud. Facebook's Privacy Policy is indicative:

> - We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see.
> - We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.

Facebook, "Privacy Policy", last modified October 5, 2010, <http://www.facebook.com/policy.php> (last accessed December 12, 2010).

[3] While some different organizations may be willing to take proactive steps to protect user privacy (to greater or lesser extents: Barocas & Nissenbaum, *supra* 2 at p. 1) the incentives in place put user privacy preferences in strong opposition to the primary purposes of the organization itself. See, for example, N. Wingfield, "Microsoft Quashed Effort to Boost Online Privacy", August 2, 2010, Wall Street Journal, <http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html>, detailing an internal Microsoft dispute over an attempt to prevent third party tracking by default in Internet Explorer 8.

[4] "Defeating the Cookie Monster: How Firefox can Improve Online Privacy", June 2, 2010, Boriss' Blog, <https://jboriss.wordpress.com/2010/06/02/defeating-the-cookie-monster-how-firefox-can-improve-online-privacy/>. See also J. Angwin & T. McGinty, "Sites Feed Personal Details to New Tracking Industry", July 30, 2010, Wall Street Journal, <http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html>, for an attempt to describe the sheer scope of online tracking.

[5] See O. Tene, "Privacy: The Next Generation", (Oxford: Oxford University Press, 2010), <http://ssrn.com/abstract=1710688>, p. 3. See also Barocas & Nissenbaum, *supra* 2, and H.W. Jenkins Jr., "Google and the Search for the Future", August 14, 2010, Wall Street Journal, <http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html>, which notes that the objective of behavioural targeting is to "know roughly who you are, roughly what you care about, roughly who your friends are", as well as where you are, now that geo-locational data is available.

[6] OPC Draft Report, *supra* 1 at p. 17. See also Barocas, *supra* 2 at p. 3.

[7] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", December 2010, <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>, p. 20.

[8] FTC, *supra* 7. See also Council of Europe, *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling,* adopted November 23, 2010, <https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>, which requires member states to take active steps to ensure online tracking/profiling is not done without "free, specific and informed consent" (s. 3.4(b)). The recommendation further prohibits the collection of sensitive data for profiling purposes except where necessary to provide the service in question (s. 3.11). UK All Party Parliamentary Communications Group, "Can we Keep Our Hands Off the Net?", October 2009, <http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf>, at para. 107 and, at para. 117:

> We recommend that the Government review the existing legislation applying to behavioural advertising, and bring forward new rules as needed, to ensure that these systems are only operated on an explicit, informed, opt-in basis.

[9] Some (Managing Director of Facebook Canada Robert Jordan) have referred to a 'customer right to personalized messaging from marketers': E. Chung, "Consumers Want Targeted Marketing: Facebook", November 30, 2010, CBCNews, <http://www.cbc.ca/technology/story/2010/11/30/facebook-targeted-marketing.html>. Others (Disney CEO Robert Iger) have stated that, by responding to online advertisements, shoppers are "essentially giving their permission to marketers to learn their habits and respond accordingly": J. Turow, J. King, C.J. Hoofnagle, A. Bleakley, & M. Hennessy, "Americans Reject Tailored Advertising and Three Activities That Enable It", September 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214>.
[10] M. Hartley, "Saturday Interview: Facebook Canada's Louise Clements", March 19, 2010, Financial Post, <http://www.financialpost.com/story.html?id=2703792>.
[11] Bill C-28, *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, 3rd session, 40th Parliament, 59 Elizabeth II, 2010, <http://www2.parl.gc.ca/content/hoc/Bills/403/Government/C-28/C-28_3/C-28_3.PDF>.
[12] J. Turow, J. King, C.J. Hoofnagle, A. Bleakley, & M. Hennessy, "Americans Reject Tailored Advertising and Three Activities That Enable It", September 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214>.
[13] E.C. Baig, "Internet Users Say, Don't Track Me", December 14, 2010, USA Today, <http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm>. For a description of Ad Networks and Ad Exchanges, see Barocas & Nissenbaum, *supra* 2, p. 2.
[14] OPC Draft Report, *supra* 1 at p. 13. See also UK All Parliamentary Group, *supra* 8, para. 107.
[15] FTC, *supra* 7, p. 21:

> These developments can provide enormous benefits to consumers, including instant, around-the-clock access to products and services, more choices, lower prices, personalized content, and the ability to communicate and interact with family, friends, and colleagues located around the globe. Consumers are using these new products and services at remarkable rates. The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer data. At the same time, the enhanced ability to collect and store consumer data has increased the risks that data will be shared more broadly than understood or intended by consumers or used for purposes not contemplated or disclosed at the time of collection.

See also, J. Brodkin, "The Price of Free Internet: a Piece of Your Soul", August 3, 2010, PCWorld, <http://www.pcworld.com/businesscenter/article/202448/the_price_of_free_internet_a_piece_of_your_soul.html>.
[16] S. Stecklow & P. Sonne, "Shunned Profiling Technology on the Verge of Comeback", November 24, 2010, Wall Street Journal, <http://online.wsj.com/article/SB10001424052748704243904575630751094784516.html>, detailing two companies that offer Canadian customers 'free' services such as, perhaps ironically, spyware and malware detection in exchange for consent to track their online activities in order to serve them tailored advertisements. M. Kirkpatrick, "Your Income, Home Ownership & Parenthood Status Now Available as an API", November 24, 2010, ReadWriteWeb, <http://www.readwriteweb.com/archives/your_income_home_ownership_parenthood_status_privacy_api.php> describes the practices of a company named 'RapLeaf', which places what some would consider sensitive financial and other information about individuals onto its API. See also Apple's recent decision to opt its users in to the geo-locational component of its new mobile advertisement system: S. Hill, "Apple Defends Opt-Out Privacy Policies in Letter to Congressmen", July 20, 2010, MacNewsWorld, <http://www.technewsworld.com/story/70449.html?wlc=1292368167>.
[17] FTC, *supra* 7, Council of Europe, *supra* 8, UK All Party Parliamentary Communications Group, *supra* 8.

[18] This design imperative has always been ignored by browsers. D. Kristol & L. Montulli, *RFC 2109: HTTP State Management Mechanism*, October 2000, Network Working Group: <http://tools.ietf.org/html/rfc2965> at section 3.3. User-Agents (browsers) are directed to reject setting or viewing of any cookie not sent directly by the primary domain. Indeed, the initial specification for cookies clearly viewed 'tracking' as an illegitimate use, even when conducted by first parties across their own websites:

> An origin server could create a Set-Cookie2 header to track the path of a user through the server. Users may object to this behavior as an intrusive accumulation of information, even if their identity is not evident. (Identity might become evident, for example, if a user subsequently fills out a form that contains identifying information.) This state management specification therefore requires that a user agent give the user control over such a possible intrusion, although the interface through which the user is given this control is left unspecified. However, the control mechanisms provided SHALL at least allow the user:
>
> - to completely disable the sending and saving of cookies.
> - to determine whether a stateful session is in progress.
> - to control the saving of a cookie on the basis of the cookie's Domain attribute.

[19] For a comparison of anti-tracking mechanisms that are possible to implement at the browser and adoption rates of these across browsers, see Center for Democracy & Technology, "Browser Privacy Features: A Work in Progress", Version 3.0, December 2010, <http://cdt.org/files/pdfs/20101209_browser_rpt.pdf>.

[20] *Ibid.* Apple's Safari browser, for example, blocks all third-party cookies by default. Mozilla is attempting to develop a more nuanced approach that differentiates between third-party cookies intended for tracking and those necessary for an optimal user experience. This solution will limit retention of third-party cookies to per-tab sessions: "Defeating the Cookie Monster: How Firefox can Improve Online Privacy", June 2, 2010, Boriss' Blog, <https://jboriss.wordpress.com/2010/06/02/defeating-the-cookie-monster-how-firefox-can-improve-online-privacy/>. Microsoft, as well, as developed solutions to third-party cookie tracking, although these have not been implemented by default: N. Wingfield, "Microsoft Quashed Effort to Boost Online Privacy", August 2, 2010, Wall Street Journal, <http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html>.

[21] FTC, *supra 7*, p. vii.

[22] FTC, *supra* 7, p. 66.

[23] J. Lo, "A 'Do Not Track List' for Canada?", October 2009, Public Interest Advocacy Centre, <http://www.piac.ca/files/dntl_final_website.pdf>, pp. 26, 50.

[24] FTC, *supra* 7, p. 68. CIPPIC has been a proponent of granular consumer controls in the past. However, it is concerned that if organizations are left to define the scope of such granularity, customers will be left with all or nothing 'take it or leave it' models that do not facilitate customer choice (see: OPC, "Letter from OPC to CIPPIC outlining its Resolution with Facebook", August 25, 2009, <http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm>. See as well CIPPIC, "Statement of Concern", February 20, 2009, <http://www.cippic.ca/uploads/Facebook-Statement_of_Concern-FINAL.pdf>, pp. 70-72.

[25] W. Davis, "Flash Cookies Could Become Hot-Button Privacy Issue", Media Post News, January 15, 2010, available online at: <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=120673>, and A. Soltani, S. Canty, Q. Mayo, L. Thomas & C. Hoofnagle, "Flash Cookies and Privacy", 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.

[26] Lo, *supra* 23, pp. 26, 50.

[27] Alternatively, CDT, *supra* 19 provides an overview of browser-based mechanisms that may make online tracking very difficult for third parties based on current tracking practices. However, it is unlikely that it is possible to prevent a determined tracker altogether: T. Vega, "New Web Code Draws Concern Over Privacy Risks" October 10, 2010, New York Times, <http://www.nytimes.com/2010/10/11/business/media/11privacy.html>, detailing how HTML5 will require providing websites (including third party websites) with significant local storage capacity on user computers. J. Cheng, "Advertisers Get Hands Stuck Inside HTML5 Database Cookie Jar", September 2010, Ars Technica, <http://arstechnica.com/apple/news/2010/09/rldguid-tracking-cookies-in-safari-database-form.ars>, detailing an investigation of a company that was using HTML5 data storage space on users computers to recreated deleted tracking cookies.

[28] CDT, *supra* 19.
[29] Facebook, Privacy Policy, *supra* 2.
[30] Google, "Privacy Policy", Last modified October 3, 2010, <http://www.google.com/intl/en/privacy/privacy-policy.html> (accessed December 12, 2010).
[31] Amazon.ca, "Privacy Notice", Last modified August 14, 2007, <http://www.amazon.ca/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=918814> (accessed December 12, 2010).
[32] K. Jebbia, "Is Google's Algorithm Changing to Consider User Behavior?", October 8, 2008, Articlesbase, <http://www.articlesbase.com/seo-articles/is-googles-algorithm-changing-to-consider-user-behavior-595266.html>.
[33] P. Wong, "Conversations About the Internet #5: Anonymous Facebook Employee", January 11, 2010, The Rumpus, <http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/>.
[34] N. O'Neil, "Facebook Knows that Your Relationship Will End in a Week", May 17, 2010, All Facebook, <http://www.allfacebook.com/facebook-knows-that-your-relationship-will-end-in-a-week-2010-05>.
[35] Office of the Privacy Commissioner, "Preliminary Letter of Findings", October 19, 2010, <http://www.priv.gc.ca/wn-qdn/index_e.cfm>.
[36] Facebook, Privacy Policy, *supra* 2.
[37] See K. Cameron, "Gov 2.0 and Facebook 'Like' Buttons", December 8, 2010, Identity Weblog, <http://www.identityblog.com/?p=1161>. See also CIPPIC, "Statement of Concern", *supra* 24, pp. 86-90.
[38] *Ibid*. Mr. Cameron concludes with respect to this practice that "The design is about as invasive of your privacy as you can possibly get."
[39] Barocas & Nissenbaum, *supra* 2, p. 3.
[40] Facebook, "What Information Does Facebook Receive About Me When I Visit a Website with a Facebook Social Plug In?", Facebook Help Center, <https://www.facebook.com/help/?faq=17512>, (accessed December 12, 2010):

> When you visit a partner site, Facebook sees the date and time you visited, the web page you are on (commonly known as the URL), and other technical information about the IP address, browser, and operating system you use. This is industry standard data that helps us optimize your experience depending on which browser you are using or letting us know that you are logged into Facebook. If you are logged into Facebook, we also see your user ID number. We need your user ID to be able to show you the right social context on that site. For example, when you go to a partner website, we need to know who you are in order to show you what your Facebook friends have liked or recommended. If you log out of Facebook, we will not receive this information about partner websites but you will also not see personalized experiences on these sites.
>
> We do not share or sell the information we see when you visit a website with a Facebook social plugin to third parties and we do not use it to deliver ads to you. In addition, we will delete the data (i.e., data we receive when you see social plugins) associated with users in 90 days. We may keep aggregated and anonymized data (not associated with specific users) after 90 days for improving our products and services. This is consistent with standard industry practice.

[41] *Ibid*.
[42] Barocas & Nissenbaum, *supra* 2, p. 4. See also Turow *et. al., supra* 12.
[43] The risk of de-anonymization is, in CIPPIC's view, likely to be higher where an organization has access to very detailed profiles reflecting individual's real life identity and practices, as Facebook has. CIPPIC additionally questions whether any retention of such data is valid for the purpose of tracking exposure to Facebook's 'like' button and other Open Graph API services, particularly where the user is not even logged in to their Facebook account while browsing.
[44] See, for examples, P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>, T. Scassa & L.M. Campbell, "Data Protection, Privacy and Spatial Data", forthcoming in *6th International Symposium on Spatial Data Quality*, 2011, for the effects that seemingly anonymous geolocational data may have on anonymity, K. El-Emam & P. Kosseim, "Privacy Interests in Prescription Data, Part 2: Patient Data", in E.M. Powers & R.L. Trope, *Eds.*, *Privacy Interests*,

March/April 2009, <http://www.ruor.uottawa.ca/fr/bitstream/handle/10393/12985/El_Emam_Khaled_2009_Privacy_interests_in_prescription_data_2.pdf>, and Privacy Analytics, "De-Identification: Reduce Privacy Risks When Sharing Personally Identifiable Information", 2009, Privacy Analytics Inc., <http://www.ehealthinformation.ca/documents/de-idwhitepaper.pdf>, for misperceptions of 'anonymity' with respect to identifiers such as postal codes in the medical research context.

[45] Paragraph s. 4(2)(c) of PIPEDA excludes personal information collected for journalistic, artistic, or literary purposes from the scope of Part 1 of the Act, meaning, significantly, that section 5(3) of PIPEDA does not apply.

[46] T. Scassa, "Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets and Location Maps", (2010) 35 Queen's L.J. 733, p. 779.

[47] See, for example, *Campbell v. MGN Ltd.*, [2004] 2 AC 457 (U.K. H.L.) and *Murray v. Express Newspapers plc and another*, [2008] All ER 70 (U.K. C.A. Civ.), both of which applied the tort of invasion of privacy to newspapers. The test applied in such scenarios by the UK courts is one that first asks whether a reasonable expectation of privacy has been invaded and, if so, balances the level of invasiveness against the expressive value of the content disclosed in the news article. In this way, the UK courts have, much as Professor Scassa and Canadian courts in a number of contexts, reconciled constitutional rights to privacy and free expression. The European Court of Human Rights has adopted a similar balancing test.

[48] See *Somwar v. McDonald's Restaurant of Canada*, [2006] 263 D.L.R. (4th) 752 (Ont. S.C.):

> With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests by providing a common law remedy for their violation would be consistent with Charter values and an "incremental revision" and logical extension of the existing jurisprudence.

[49] OPC, PIPEDA Case Summary #2009-008, *supra* 2 at para. 211.4. See also OPC, Letter of Resolution, *supra* 24.

[50] See Facebook, "Places: Who. What. When. And now Where.", Facebook.com, <https://www.facebook.com/places/>, (accessed December 12, 2010).

[51] OPC, Draft Report, *supra* 1 at pp. 15-16.

[52] OPC, Draft Report, *supra* 1 at p. 23, noting that, even where information on behavioural targeting is made accessible, the practice itself "is fairly complex and would be difficult to explain".

[53] PIPEDA, Principles 4.3.4, 4.3.5 & 4.3.6.

[54] PIPEDA Case Summary #2009-008, *supra* 2, para. 89. See also OPC, Draft Report, *supra* 1 at p. 26.

[55] CIPPIC, Statement of Concern, *supra* 24.

[56] *Ibid*.

[57] EU the Telecommunications Commissioner Viviane Reding described her response to these changes as one of "astonishment", noting that "[a]ll of sudden there is a complete change of policy…I can't understand that because it's in the interest of the social network sites to give users control of their privacy."(M. Newman, "Facebook's Privacy Changes Being Watched by European Commission", Business Week, February 5, 2010, <http://www.businessweek.com/news/2010-02-05/facebook-s-privacy-changes-being-watched-by-european-commission.html>). See also: I. Kerr, "The Devil is in the Defaults", May 29, 2010, Ottawa Citizen – Citizen Special, <http://www.iankerr.ca/>, CIPPIC, Statement of Concern, *supra* 24.

[58] J. Kincaid, "Apple Announces iAd Advertising Platform", April 8, 2010, TechCrunch, <http://techcrunch.com/2010/04/08/apple-announces-iad-mobile-advertising-platform/>, and B. Sewell, "Apple Inc.s Response to Request for Information Regarding Its Privacy Policy and Location-Based Services", July 12, 2010, <http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf>. Contrast this position with: N. O'Neil, "Steve Jobs Offers His Opinion on Privacy at D8", June 1, 2010, All Facebook, <http://www.allfacebook.com/steve-jobs-offers-his-opinion-on-privacy-at-d8-2010-06>: "Some people want to share more data. Ask them. Ask them every time. Let them know precisely what you are going to do with their data."

[59] Letter to Google Inc. Chief Executive Officer, April 19, 2010, Office of the Privacy Commissioner, <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm>.
[60] OPC Draft Report, *supra* 1, p. 26.
[61] *Ibid*., p. 16.
[62] FTC, *supra* 7, p. 60. For the social networking context, see: Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, [EU Working Group] (2009) 01189/09/EN, WP 163, <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf>, p. 7.
[63] Lo, *supra* 23, p. 12.
[64] For an example of this type of one-off, take it or leave it exchange, see FIGURE E-1, which presents a screenshot of the authentication window a user must accept if seeking to sign in to the Huffington Post using Facebook. Users must provide the Post with access to a fairly broad amount of personal information (which it then uses to serve them with targeted advertisements) in order to register. There is no option to limit the degree of access the Post will get to only what it requires (i.e. user name).
[65] R. Dhamija & L. Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges", (2008) March/April *IEEE Security & Privacy* 24, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4489846> at p. 26, with respect to Microsoft's Cardspace Identity Management interface. See also I. Kerr, J. Barrigar, J. Burkell, & K. Black, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent", in I. Kerr, V. Steeves, & C. Lucock, *Eds*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799> and A. Acquisti & J. Grossklags, "Privacy and Rationality in Individual Decision Making", (2005) January/February *IEEE Security & Privacy* 26, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1392696&userType=&tag=1>.
[66] CIPPIC, Statement of Concern, *supra* 24, pp. 62-67.
[67] The latest example being Facebook's introduction of facial recognition software on its site. Users are provided with the option of opting themselves out of automatic facial recognition if they wish (J. Mitchell, "Making Photo Tagging Easier", December 15, 2010, The Facebook Blog, <http://blog.facebook.com/blog.php?post=467145887130>. Other recent examples include 'Facebook Places' (Facebook's geo locational tool, which permitted users to tag other users at specific locations unless those users opted out): M.E. Sharon, "Who, What, When, and Now…Where", August 18, 2010, The Facebook Blog, <http://blog.facebook.com/blog.php?post=418175202130>; Instant Personalization (where, unless users opted out, Facebook began identifying otherwise anonymous users to a small but expanding group of external websites as soon as those users open these external websites and providing these websites with access to personal information of user): M. Zuckerberg, "Building the Social Web Together", April 21, 2010, The Facebook Blog, <http://blog.facebook.com/blog.php?post=383404517130>.
[68] CIPPIC notes that, in this respect, amendments proposed by Bill C-29 may be of great assistance.
[69] See, for examples, *BMG v. Doe*, [2005] 252 D.L.R. (4th) 342 (F.C.A.) (asking for an order against ISPs to identify customers associated with IP addresses accused of sharing materials on peer-to-peer sites in violation of the plaintiff's copyright), *York University v. Bell Canada Enterprises*, [2009] 99 O.R. (3d) 695 (Ont. S.C.) (in which action Google, Bell and Rogers were ordered to identify the York faculty member who had sent out an email to the faculty from an anonymous account criticizing a faculty decision as well as allegedly defaming another academic), and *Warman v. Fournier*, [2010] 319 D.L.R. (4th) 268 (Ont. Div. Ct.) (motion against the owners of a message board seeking identification information of anonymous individuals on that had made allegedly defamatory comments on its site).
[70] *Carter v. Connors*, [2009]355 N.B.R. (2d) 235 (N.B. Q.B.) (in which the court ordered the plaintiff's ISP to provide the defendant with records detailing the extent and times of the plaintiff's use of the internet and, more specifically, of her use of social networking site Facebook [assuming those records could be generated] in order to challenge the plaintiff's claim of physical infirmity and inability to work).
[71] *Schuster v. Royal & Sun Alliance Insurance Co.*, [2009] 83 C.P.C. (6th) 365 (Ont. S.C.), *Leduc v. Roman*, [2009] 308 D.L.R. (4th) 353 (Ont. S.C.).
[72] *BMG, supra* 69, *Warman, supra 69* and *Carter, supra* 70.
[73] Bill C-29, the *Safeguarding Canadians' Personal Information Act*, ["SCPA"] <http://www2.parl.gc.ca/content/hoc/Bills/403/Government/C-29/C-29_1/C-29_1.PDF>, see Clause 6(9).

[74] *State Farm Mutual Automobile Insurance v. Canada (Privacy Commissioner)*, [2010] 7 Admin. L.R. (5th) 77 (F.C.). Indeed, such organizations may, absent broad statutory exemptions, ultimately be subject to fiduciary duties preventing, in some circumstances, disclosure of customer information: I. Kerr, "Online Service Providers, Fidelity, and the Duty of Loyalty", in *Ethics and Electronic Information*, T. Mendina & B. Rockenbach, *Eds.*, (Jefferson, North Carolina: McFarland Press, 2002), <http://iankerr.ca/files/onlineserviceprovidersfidelityandthedutyofloyalty.pdf>.
[75] For an overview, see T. Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", (2010) Can. J. L. & Tech. 193, pp. 209-212. See also, for a review of some of the case law to date, *R. v. Cuttell*, [2009] 247 C.C.C. (3d) 424 (Ont. C.J.), paras. 20, 29. See, as well, *R. v. Gomboc*, 2010 SCC 55, S.C.C.) at paras. 32 and 93-94.
[76] The SCPA, *supra* 73 seeks to adopt and expansive definition of 'lawful authority'. This will, as Professor Scassa points out, have serious impact on protections Canadians can expect under section 8 of the *Charter* (Scassa, *supra* 75, pp. 208-209.
[77] See, specifically, Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, <http://www2.parl.gc.ca/content/hoc/Bills/403/Government/C-52/C-52_1/C-52_1.PDF>, which applies broadly to any service provided via the Internet.
[78] D. Gilbert, I. Kerr, & J. McGill, "The Medium and the Message: Personal Privacy and the Force Marriage of Police and Telecommunications Providers", (2007) 51(4) *Crim. L. Q.* 469. C. Soghoian, "8 Million Reasons for Real Surveillance Oversight", December 1, 2009, Slight Paranoia, <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html>, documents the general shift away from warrant-based disclosures and towards informal 'requests' from online intermediaries in the United States. Soghoian documents the decision of one ISP to provide law enforcement with an automated web interface so that law enforcement agents may request GPS data regarding its customers. The interface processed 8 million automated location requests on some 10,000 customers over the course of one single year. None of these requests, of course, were subject to any type of judicial oversight.
[79] *Cuttell, supra* 75, para. 31, citing Bell Canada's Internet Service Agreement.
[80] *Cuttell, supra* 75, paras. 32-33.
[81] L. Lessig, "Code 2.0", (NY: Basic Books, 2006), p. 77.
[82] Office of the Privacy Commissioner of Canada, "Identity, Privacy and the Need of Others to Know Who Your Are: A Discussion Paper on Identity Issues", September 2007, <http://www.priv.gc.ca/information/pub/ID_Paper_e.pdf> ["OPC ID Paper"], p. 31.
[83] I. Kerr, V. Steeves, & C. Lucock, *Eds*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799>, p. xxiv.
[84] C. Schultz, "Web Site Posters' Anonymity an Invitation to Mischief: Connie Schultz", March 28, 2010, Cleveland.com, <http://www.cleveland.com/schultz/index.ssf/2010/03/web_site_posters_anonymity_an.html>. Ms. Schultz is a columnist for the Cleveland 'Plain Dealer' who penned her tirade against online anonymity very soon after her paper had garnered a great deal of public attention for revealing the identity of an anonymous Doe who had made frequent comments on its online articles.
[85] *Ibid*. See also, J.F. McCarthy, "Anonymous Online Comments are Linked to the Personal e-mail Account of Cuyahoga County Common Pleas Judge Shirley Strickland Saffold", March 26, 2010, Cleveland.com, <http://blog.cleveland.com/metro/2010/03/post_258.html>. The story has attracted, at the time of this writing, 199 comments, many of an anonymous nature.
[86] *Ibid.* See also: R. Perez-Pena, "News Sites Rethink Anonymous Online Comments", April 11, 2010, New York Times, <https://www.nytimes.com/2010/04/12/technology/12comments.html>.
[87] Kerr & Barrigar *et. al. supra* 65.
[88] Perez-Pena, *supra* 86.
[89] Wall Street Journal, "Journal Community", <http://online.wsj.com/community/faq>, (accessed December 12, 2010):

> **Community Rules**
> We want everyone to benefit from this community of thoughtful peers and therefore request that you contribute thoughtful and sincere comments and content. However, there are certain mandatory rules that each person ("Member") participating in this Community must follow.

> Each Member must comply with the following rules of conduct while participating in this Community:
>
> - You must use your actual first and last name when you participate in the Community, including when posting any comments or participating in any discussions. Of course, you may not represent that you are any other person, whether real or invented, or imply any connection with any person or organization with which you are not in fact associated.

[90] Perez-Pena, *supra* 86.
[91] OPC ID Paper, *supra* 82, p. 17.
[92] CIPPIC notes that Facebook, where the majority of users operate under real-life identities (in fact, Facebook requires this), has not managed to eliminate abusive online comments. Indeed, CIPPIC receives numerous calls from individual users who have been the subject of abusive complaints on Facebook. For more high profile example, see: The Telegraph, "Buckingham Palace Forced to Remove Abusive Comments from Queen's Facebook Page", December 8, 2010, The Telegraph, <http://www.telegraph.co.uk/news/newstopics/theroyalfamily/8117351/Buckingham-Palace-forced-to-remove-abusive-comments-from-Queens-Facebook-page.html>. Note that many of the 'abusive' comments in this example were made under real names and identities, as is often the case on Facebook.
[93] The current abstention from identity verification appears to stem from a.) a belief among news executives that "merely making the demand for a name and an e-mail address would weed out much of the most offensive commentary" and b.) the fact that at this point verification is too labour intensive and unrealistic (Perez-Pena, *supra* 86). It remains to be seen whether the simple requirement of an email address-based registration process will be sufficient to deter abusive online comments, verification may soon become a fairly easy endeavour.
[94] OPC ID Paper, *supra* 82 pp. 32, 34.
[95] See Appendix A for screenshots, taken December 8, 2010.
[96] Google Accounts Help, "Frequently Asked Questions on Account Verification via SMS or Voice Call", Basics: Account Verification via SMS or Voice Call", Google Accounts > Basics: Account Verification via SMS or Voice Call, <https://www.google.com/support/accounts/bin/answer.py?answer=114129&hl=en&ctx=ch_CreateAccount&p=mail> ["Google Verification FAQ"] (accessed December 8, 2010).
[97] See Screenshot, Appendix A, *supra* 95.
[98] Google Verification FAQ, *supra* 96:

> **I don't have a phone. Can I sign up?**
> If you're trying to sign up for a Google Account, you may be asked to provide a phone number to verify your account. You'll have the option to receive a verification code by text message (SMS) or automated voice call. If you choose the text message option, make sure the phone you use has text-messaging capabilities. If you don't have a mobile phone, try using the voice call option. If you don't have a phone, ask a friend to use his or her number to receive the code via text message or voice call. If you use the voice call option, you'll receive a call and hear an automated message with a verification code. Enter the code on the page to complete the process.

[99] See *supra* 84. There are far less privacy intrusive ways to verify that the potential registrant of an email account is 'live' and not a spam 'robot'. See, for example, http://en.wikipedia.org/wiki/CAPTCHA.
[100] Appendix A, FIGURE E-1 and FIGURE E-2:.
[101] Appendix A, FIGURE E-2:.
[102] M. Ingram, "Facebook's No-Pseudonym Policy is Short-Sighted", internet evolution, November 12, 2007, <http://www.internetevolution.com/author.asp?section_id=539&doc_id=138520>.
[103] See Appendix A, FIGURE C-1.
[104] See Appendix A, FIGURE B-1 (Full) to FIGURE B-3 (Full) for screenshots. Users attempting to customize profile name/URL from Facebook's Account Settings>Settings tab ('Username') are confronted by the following message:

> **Before you can set your username, you need to verify your account.**
> If you have a mobile phone that can receive SMS message, you can verify via mobile phone. If not, please try to register your username at a later time.

[105] Appendix A, FIGURE D-1.
[106] Appendix A, FIGURE D-4.
[107] Facebook cites 'encouragement of authenticity' as its rationale for requiring a date of birth (see Appendix A, FIGURE C-2). Presumably, this rationale applies to the 'real name' requirement as well. See OPC ID Paper, *supra* 91, p. 23 for other potential reasons a real identity may be required in such circumstances.
[108] S.M. Nir, "An Online Alias Keeps Colleges Off Their Trail", New York Times, April 23, 2010, <https://www.nytimes.com/2010/04/25/fashion/25Noticed.html>, T. Hunter, "Girl's Death Shows Dangers of 'Publishing Your Life Online'", Sydney Morning Herald, August 18, 2010, <http://www.smh.com.au/technology/security/girls-death-shows-dangers-of-publishing-your-life-online-20100517-v822.html>.
[109] M. Melanson, "Facebook Wants to be Your One True Login", ReadWriteWeb.com, February 10, 2010, online: <http://www.readwriteweb.com/archives/facebook_wants_to_be_your_one_true_login.php>.
[110] J. Clark, P. Gauvin, & C. Adams, "Exit Node Repudiation for Anonymity Networks", in I. Kerr, V. Steeves, & C. Lucock, *Eds*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799>, p. 400.
[111] Much in the same manner as online advertising networks track a user across multiple sites on which the network's advertisements are present – by accessing the network's cookie through the browser. See Lo, *supra* 23.
[112] Lo, *supra* 23 at p. 26 describes how Microsoft uses such persistent, cross-platform logins in conjunction with its online advertisement services in order to conduct its behavioural targeting activities on wireline and mobile services.
[113] *Supra* 85. See also the discussion of 'Identifier Schemes' in E. Maler & D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management", (2008) March/April *IEEE Security & Privacy* 16, <http://www.xmlgrrl.com/publications/IEEESecPriv-MarApr2008-MalerReed-Venn.pdf>, p. 18.
[114] CIPPIC notes that there are legitimate and important reasons for using a single logout process in federated identity management systems such as that used by Facebook (see Maler & Reed *supra* 113, p. 18). These security concerns appear proportional where the authenticating entity, in this case Facebook, is a pure identity management provider. However, where it is a social networking entity in its own right, and where the services relying on it for registration are potentially as diverse as the web itself, there must be a process for users to utilize different identities across different sites simultaneously.
[115] Many sites, for example, permit users to register using a Facebook account although few limit registration options to Facebook *alone* yet. Once registered to a site with a Facebook account, it becomes difficult if not impossible (depending on the site) to log in to a second account while logged in to Facebook in a different tab.
[116] See Ohm, *supra* 44, Scassa & Campbell, *supra* 44 (for the effects that seemingly anonymous geolocational data may have on anonymity), El-Emam & Kosseim, *supra* 44, and Privacy Analytics, *supra* 44 (for misperceptions of 'anonymity' with respect to identifiers such as postal codes in the medical research context).
[117] See, for example, reactions to Facebook's privacy transition in December 2009, which resulted in large amounts of user data suddenly becoming 'publicly available'. As noted above, then EU Telecommunications Commissioner Viviane Reding described her reaction to Facebook's Transition changes with the term 'astonishment': Newman, *supra* 57. See also: L. Phillips, "New EU Privacy Laws Could Hit Facebook", Business Week, January 29, 2010, <http://www.businessweek.com/globalbiz/content/jan2010/gb20100129_437053.htm>, K. Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and the Ugly", Electronic Frontier Foundation, December 9, 2009, <http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>, and N. Ozer, "Facebook Privacy in Transition – But Where is it Heading?", American Civil Liberties Union, Blog of Rights, December 9, 2009, <http://www.aclu.org/blog/technology-and-liberty/facebook-privacy-transition-where-it-heading>
[118] A.M. Froomkin, "Identity Cards and Identity Romanticism", in I.R. Kerr, V. Steeves, & C. Lucock, *Eds*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799>, 245.
[119] See A. Bowie, "Issues in Identity Management", in CIPPIC, *Digital Agenda: A Plan for Canada's Digital Society*, July 14, 2010, <http://www.cippic.ca/uploads/CIPPIC-Digital_Consult-Submission-07142010.pdf>.

[120] S. Landau, H. Le Van Gong, & R. Wilton, "Achieving Privacy in a Federated Identity Management System", in R. Dingledine & P. Golle, *Eds.*, (2009) 5628 FC LNCS 51, <http://www.springerlink.com/content/b149n4u255u3n378/fulltext.pdf>.
[121] Dhamija & Dusseault *supra* 65, p. 24: "The challenges involve dependencies, complex trade-offs, and sometimes even contradictory design requirements, and therefore must be addressed in an integrated fashion." See also, K. Cameron, "The Laws of Identity", May 12, 2005, Kim Cameron's Identity Weblog, <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>, ["Cameron, Laws"], p. 7.
[122] Landau *et. al.*, *supra* 120, p. 63, especially, describes the deliberate line between policy/regulatory solutions and technical solutions drawn into the design of the Liberty Identity Federation specifications.
[123] Landau *et. al., supra* 120, p. 64; Dhamija & Dusseault, *supra* 65, p. 26, Acquisti & Grossklags, *supra* 65.
[124] Center for Democracy & Technology, "Issues for Responsible User-Centric Identity", November 2009, v. 1.0, <http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf>, p. 1.
[125] *Ibid*.
[126] *Ibid.*, p. 2.
[127] This basic entity description is from Maler & Reed *supra* 113, p. 17.
[128] Landau *et. al., supra* 120, p. 64.
[129] Maler & Reed *supra* 113, p. 21.
[130] See Landau *et. al., supra* 120, generally.
[131] Maler & Reed *supra* 113, p. 22.
[132] Dhamija & Dusseault *supra* 65, p. 25. See also Appendix A, FIGURE E-1.
[133] The Public Voice, "Civil Society Background Paper", Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition, <http://www.oecd.org/dataoecd/45/47/44686738.pdf>, ["Civil Society Backgrounder"].
[134] Civil Society Backgrounder, *supra* 133, p. 30. See also OPC ID Paper, *supra* 82 at p. 32: "…unless there is a valid reason for requiring individuals to identify themselves, the right to anonymity should be the norm. The right to anonymity is the highest right individuals should have, and it should be overruled only for justifiable reasons."
[135] CIPPIC, Statement of Concern, *supra* 24, pp. 62-68. See also Dhamija & Dusseault, *supra* 65, p. 28: "User consent could lead to maximum information disclosure."
[136] Civil Society Backgrounder, *supra* 133, To avoid this type of linkability, the Liberty Alliance SAML protocols, for example, utilize case-specific pseudonyms that only are only meaningful to the IdP and SP in question. That is, these pseudonymous identifiers are unique per IdP-SP interaction (and, potentially, across different IdP-SP transactions): G.-J. Ahn & J. Lam, "Managing Privacy Preferences for Federated Identity Management", in V. Atluri, P. Samarati, & A. Goto, *Chairs*, (2005) *Digital Identity Management '05: Proceedings of the 2005 ACM Workshop on Digital Identity Management* 28, <http://portal.acm.org/citation.cfm?id=1102492>, p. 30.
[137] Maler & Reed *supra* 113, p. 18. Cameron, Laws *supra* 121, p. 7: "…unique identifiers that can be reused in other contexts…represent 'more identifying information' than unique special-purpose identifiers that do not cross context." (my emphasis).
[138] See Clark *et. al. supra* 110.
[139] Landau *et. al.*, *supra* 120, p. 62.
[140] See CDT, *supra* 124, p. 4. The 'identity selector' user-agent interface in the InfoCard/Cardspace IdM specification acts as a go-between the IdP and the relying party/service provider. It may be implemented in a manner that will let users hide their online browsing activities from the IdP: Maler & Reed, *supra* 113, p. 22.
[141] Civil Society Backgrounder, *supra* 133.
[142] Dhamija & Dusseault *supra* 65, p. 26.
[143] See *infra* pp. 6-7 for a discussion of the issues that arise where a service provider is permitted to unilaterally change its service in significant ways without seeking *robust* user consent.
[144] Civil Society Backgrounder, *supra* 133.
[145] See Maler & Reed *supra* 113, p. 23.
[146] Y. Wong, "What's Wrong with OpenID?", Quora, April 14, 2010, <http://www.quora.com/What-s-wrong-with-OpenID>. It should be noted, with respect to OpenID, that it is moving away from a URL based approach and to support of more intuitive XRI sequences: Maler & Reed *supra* 113, p. 21.

[147] Damija & Dusseault *supra* 65, p. 27. Although even the most consistent and secure of interfaces may be compromised by 'safe' service providers who later turn rogue, so it remains important to provide each service provider with unique identifiers and as little information as possible.
[148] J. Shende, "Identity Management in Cloud Computing", August 31, 2010, Cloud Computing Journal, <http://cloudcomputing.sys-con.com/node/1516437>.
[149] Landau *et. al.*, *supra* 120, p. 62 call for non-aggregation as a default, with a potential opportunity to seek opt-in consent in some cases.
[150] Damija & Dusseault *supra* 65, p. 26, point out that while Cardspace, an implementation of the InfoCard protocols, permits users to 'edit' the information included in an 'identity' requested by a service provider before sending it, few users are likely to take the steps to do that. The concern is that, since users are not required to expressly select the specific items they are being asked to provide, they will become accustomed to simply providing whatever information is contained in the pre-packaged identity the service provider requests, regardless if its overbroad. For a visual example, see Appendix A, FIGURE E-1.
[151] Landau *supra* 120, p. 64: "Identity-management systems derive both strength and legitimacy from the consent of the individual whose PII is being used."
[152] See *supra* note 57.
[153] Cameron, Laws, *supra* 121, p. 6, cautioning against arbitrary unilateral changes of contract.
[154] Cameron, Laws, *supra* 121, p. 6.
[155] Maler & Reed *supra* 113, p. 23 describe in brief the development of such standards by Identity Commons.
[156] See *infra*, Section III.A: Obligations to Self-Identify, pp. 10-13.

APPENDIX A - SCREENSHOTS

A. Gmail Mandatory SMS/Voice Verification

Screenshots taken December 8, 2010, while attempting to open anonymous Gmail Account, Tamir Israel

FIGURE A-1

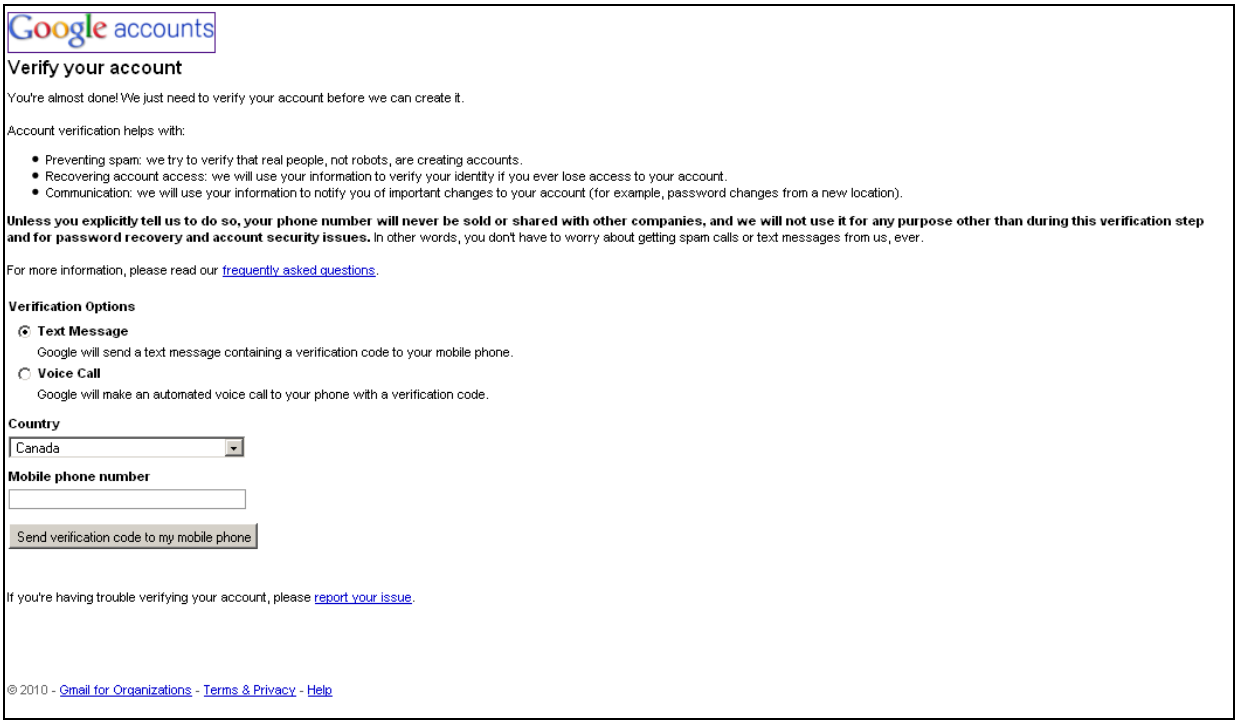


FIGURE A-2 (report your issue)

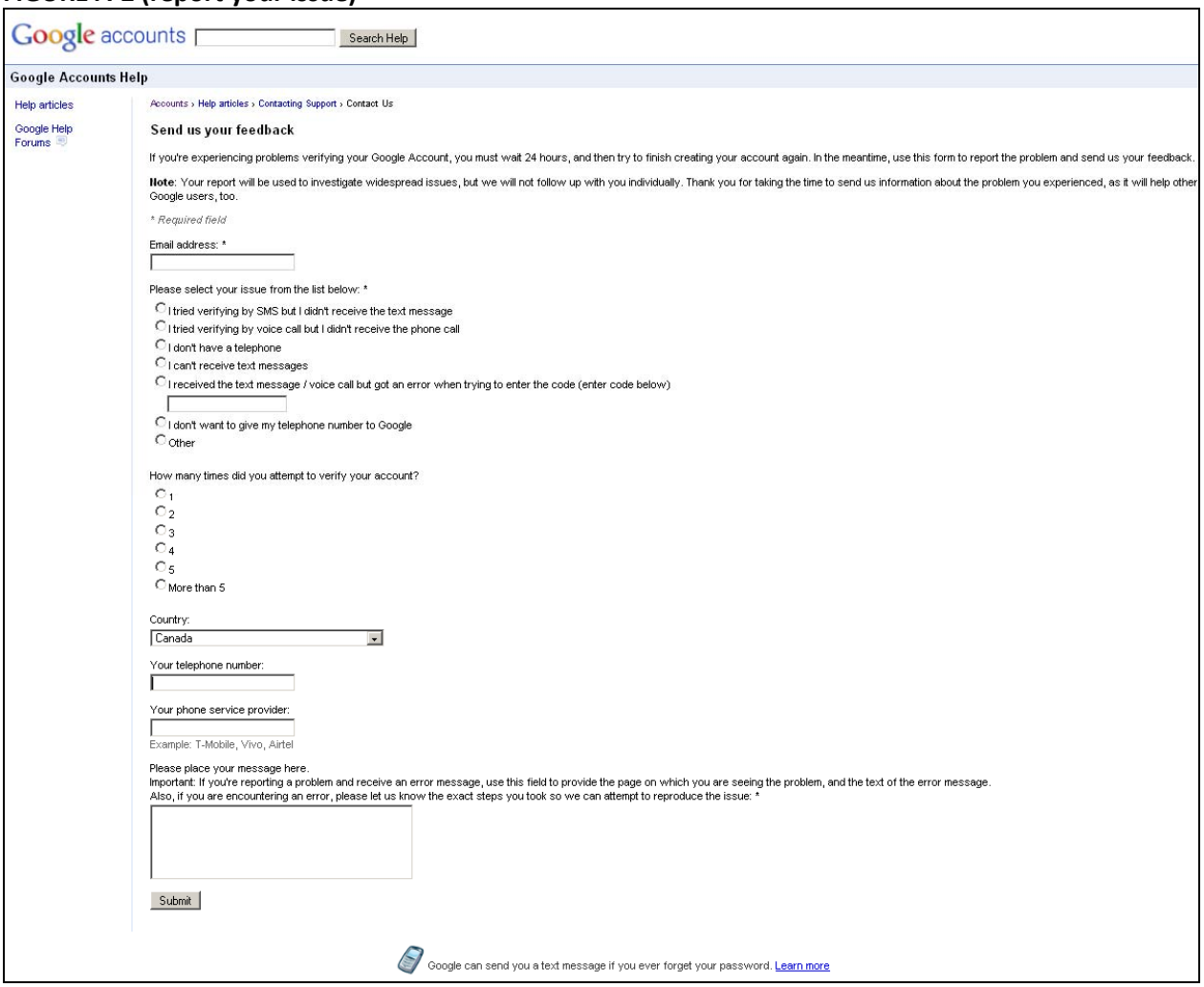
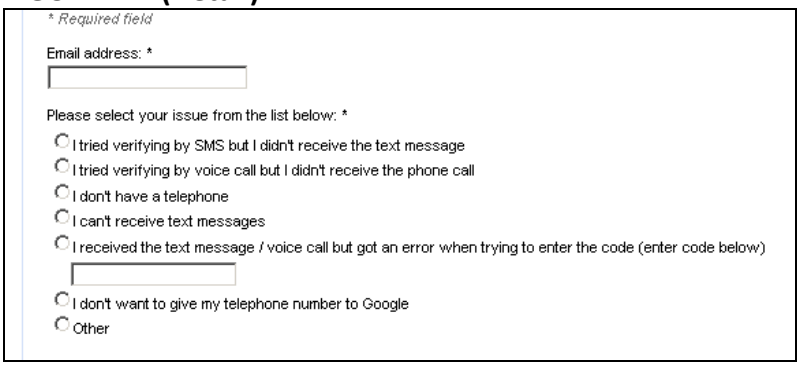


FIGURE A-2 (Detail)



B. Facebook Mandatory SMS Verification (Customized URL)

Screenshots taken December 8, 2010, while attempting to select a customized user name/URL on Facebook, Tamir Israel

FIGURE B-1 (Full)

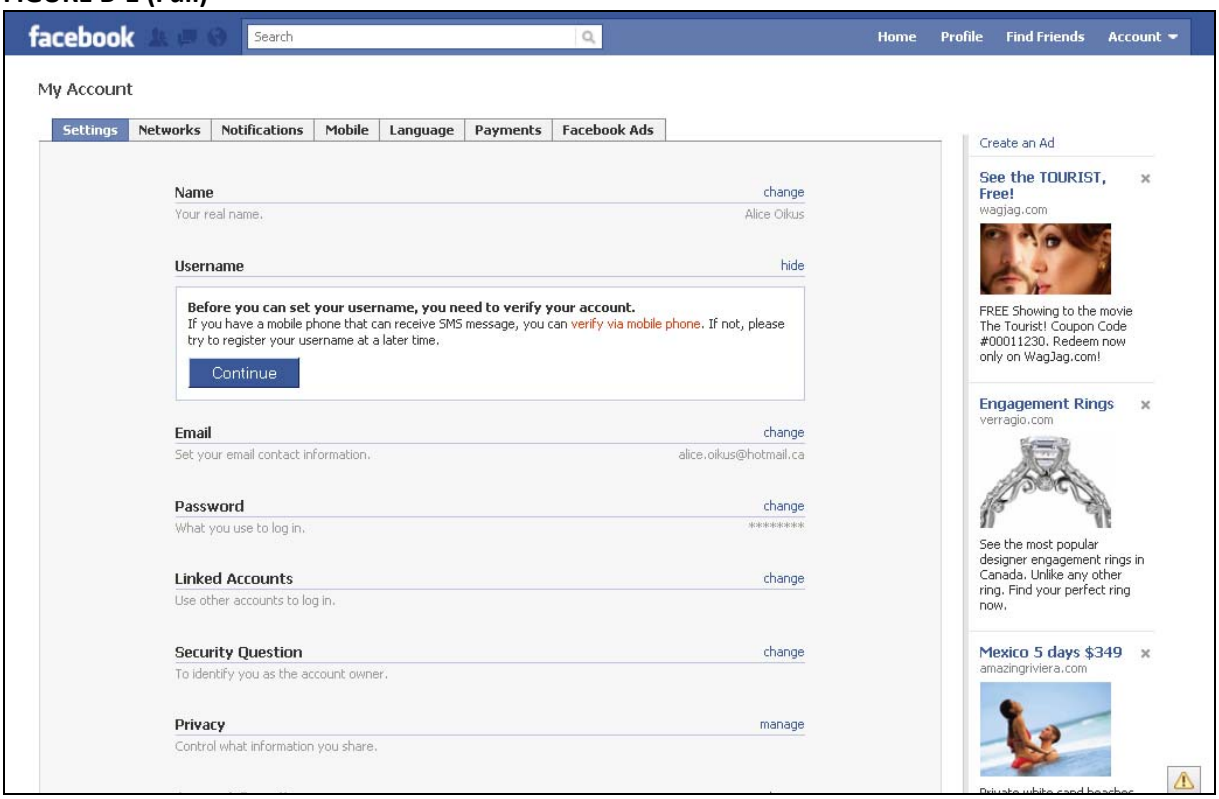


FIGURE B-1 (Detail)

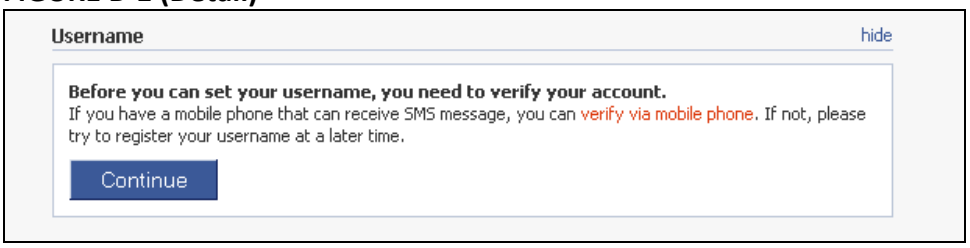


FIGURE B-2 (Full)

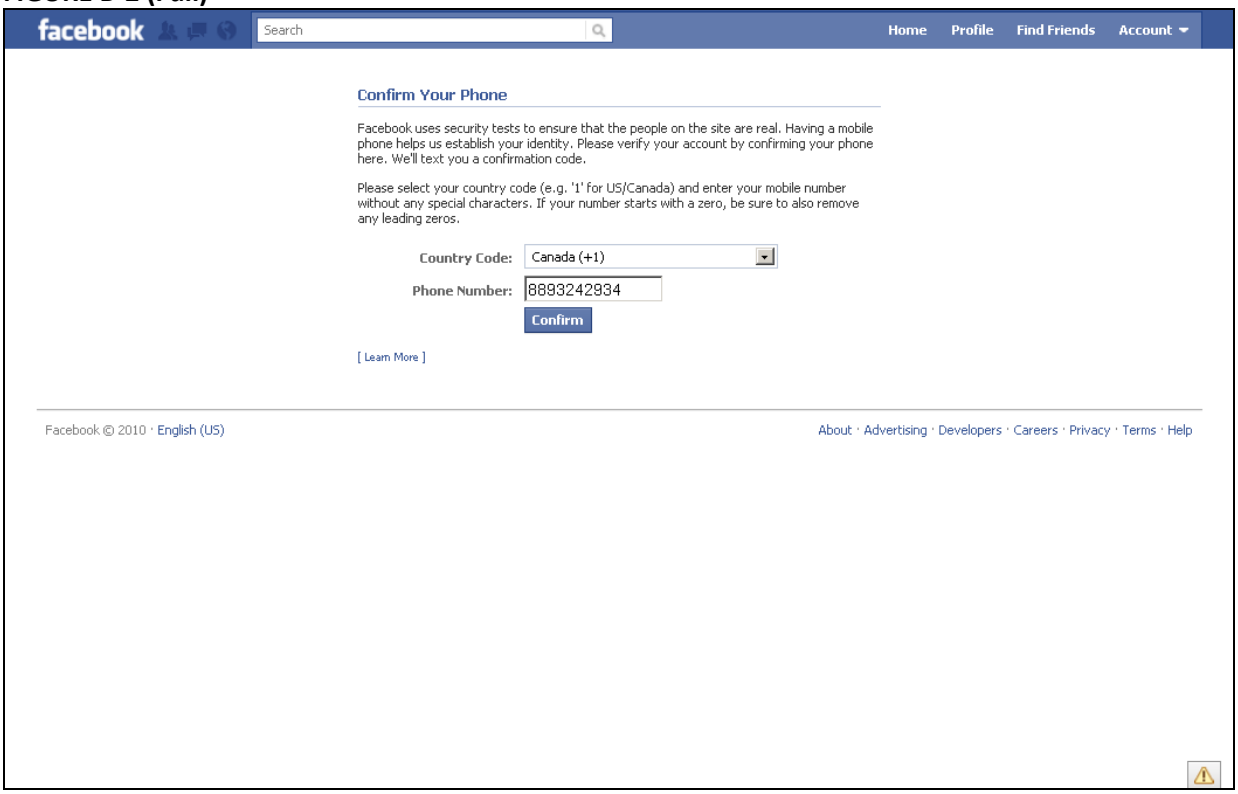


FIGURE B-3 (Full)

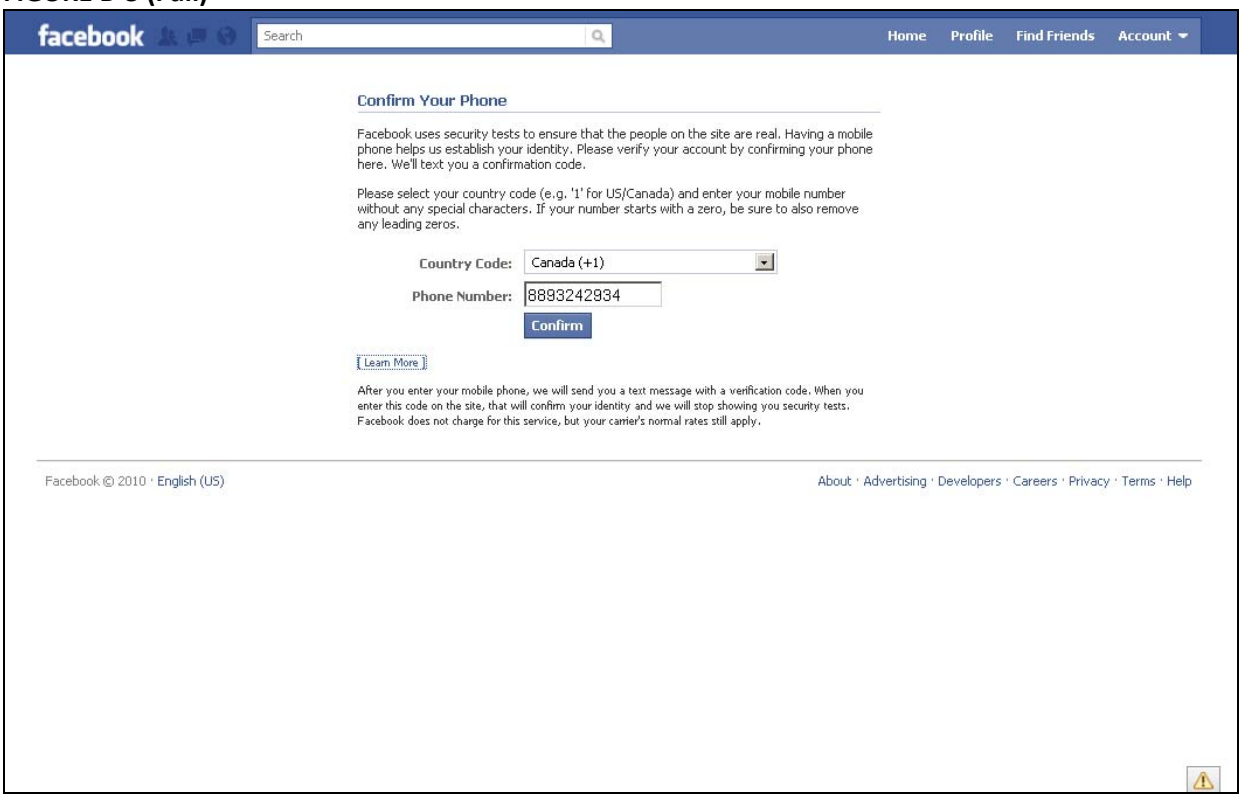
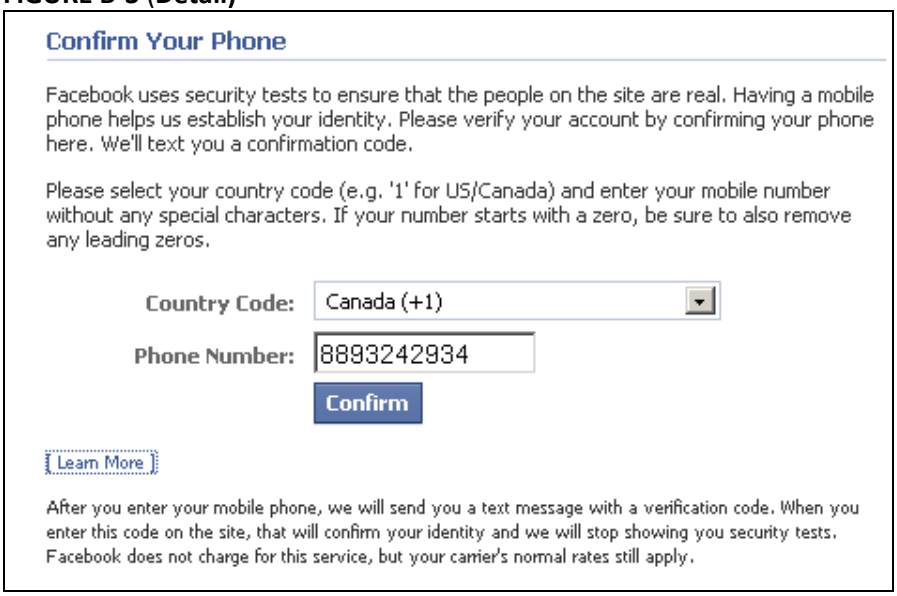


FIGURE B-3 (Detail)

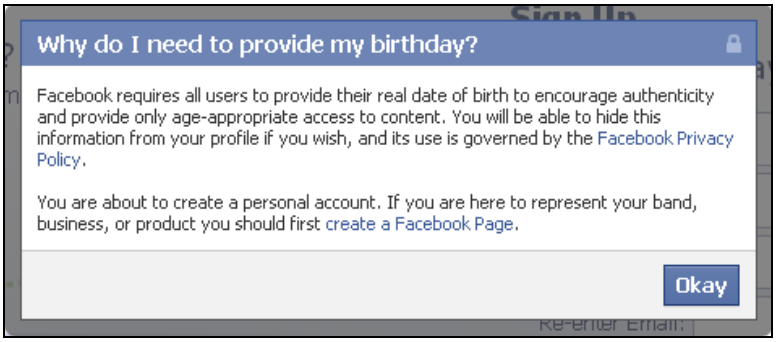


C. Facebook Name Change

Screenshots taken December 8, 2010, while attempting to select a change my first name on Facebook, Tamir Israel

FIGURE C-1

FIGURE C-2



D. Facebook 'Update Your Security' Prompt

Screenshots taken December 11, 2010, when prompted after logging in to user account.

FIGURE D-1 User is directed to this screen upon login

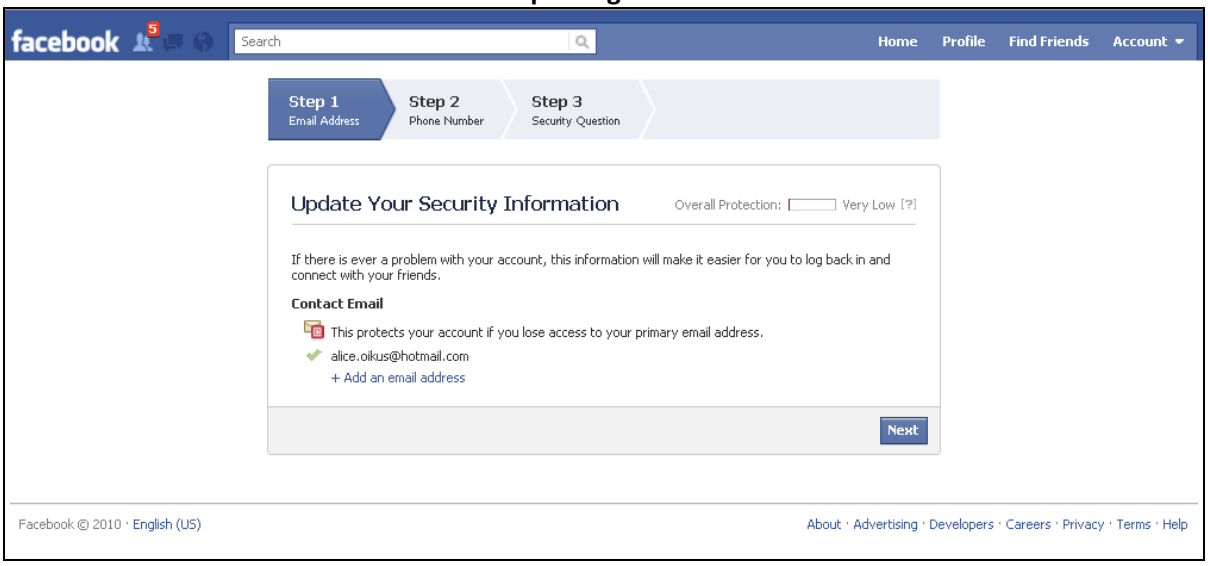


FIGURE D-2

FIGURE D-3

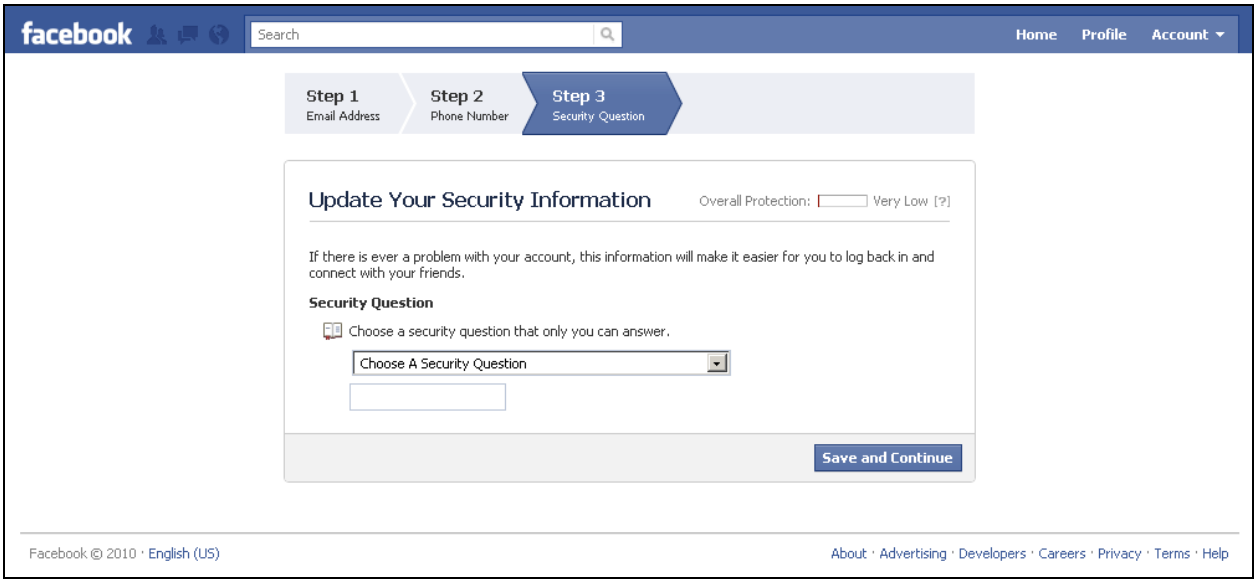
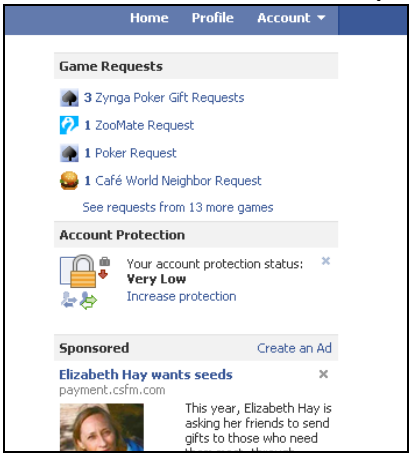


FIGURE D-4 PopUp at end of process

FIGURE D-5 Sidebar Reminder (Later, December 20, 2010)



E. ‘Connecting’ to the Huffington Post

Screenshots taken December 12, 2010.

FIGURE E-1

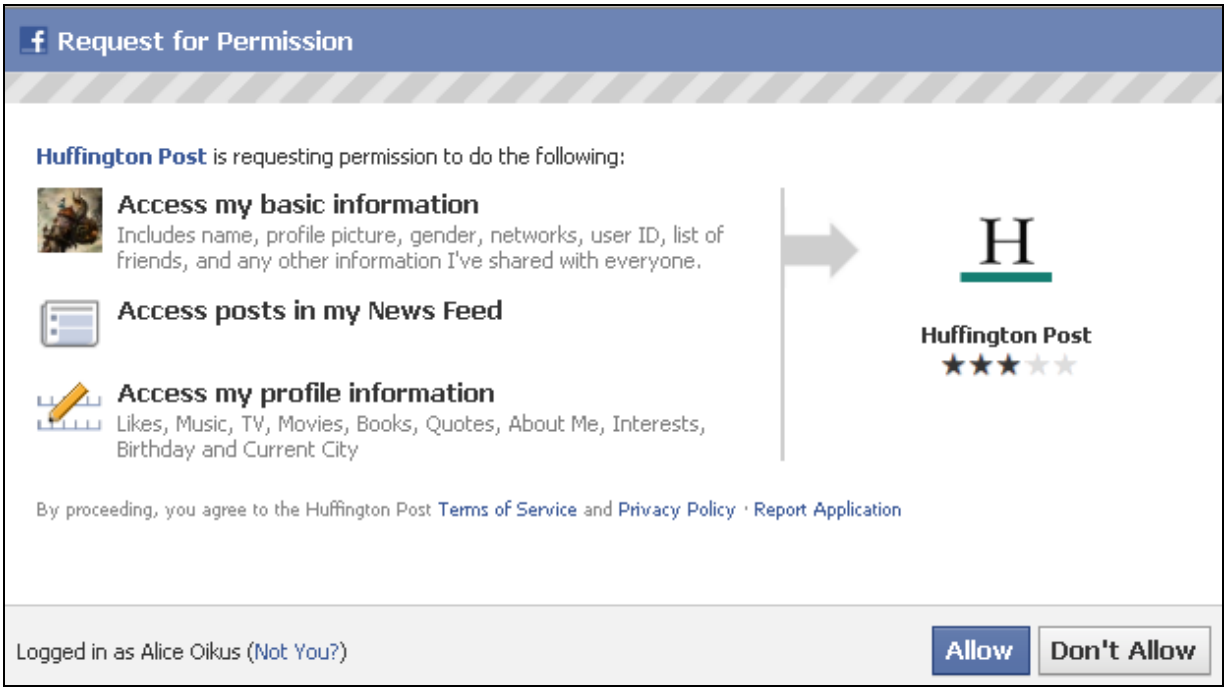


FIGURE E-2: