PRIVACY INVASIVE GEO-MASHUPS: PRIVACY 2.0 AND THE LIMITS OF FIRST GENERATION INFORMATION PRIVACY LAWS

Mark Burdon†

ABSTRACT

Online technological advances are pioneering the wider distribution of geospatial information for general mapping purposes. The use of popular web-based applications, such as Google Maps, is ensuring that mapping based applications are becoming commonplace amongst Internet users which has facilitated the rapid growth of geo-mashups. These user-generated creations enable Internet users to aggregate and publish information over specific geographical points. This article identifies privacy invasive geo-mashups that involve the unauthorized use of personal information, the inadvertent disclosure of personal information and invasion of privacy issues. Building on Zittrain's Privacy 2.0, the author contends that first generation information privacy laws, founded on the notions of fair information practices or information privacy principles, may have a limited impact regarding the resolution of privacy problems arising from privacy invasive geo-mashups. Principally because geo-mashups have different patterns of personal information provision, collection, storage and use that reflect fundamental changes in the Web 2.0 environment. The author concludes by recommending embedded legal, organizational technical and social solutions to minimize the risks arising from privacy invasive geo-mashups that could lead to the establishment of guidelines to assist courts and regulators with the protection of privacy in geo-mashups.

† PhD Candidate and Research Associate, Faculty of Law and Information Security Institute, Queensland University of Technology. The author gratefully acknowledges funding support from the Smart Services Cooperative Research Centre and the Queensland Government Department for State Development. The author would like to thank Roger Clarke and an anonymous reviewer for their helpful comments on previous drafts.

I. INTRODUCTION

There are now over one billion Internet users worldwide.[1] The wider availability of high-speed broadband[2] has facilitated greater levels of information sharing and culminated in the second generation of the Internet, often labeled as Web 2.0.[3] Consequently, Internet users now create, store and publish more information online.[4] The social networking site, Facebook, has published online over fifteen billion photographs uploaded by the site's user community.[5] Facebook publishes an average of 220 million new photographs each week and at its busiest, Facebook can publish around 550,000 photographs per second.[6] Contemporary Internet environments have propagated new online technologies and sources of data, which culminates in new technical, social, and economic structures. Different types of information are now available that can be easily re-composed into new content. The increased availability of geospatial information is a prime example. Geobrowsers[7] now make it easier for Internet users to create geo-mashups, individualized and specialized maps that use freely available, or user generated information. For the purpose of this article, a geo-mashup[8] is defined as an information system that combines one or more data streams that is overlaid on an online geographical interface, to create original content.[9]

The numbers of geo-mashups continue to rise inexorably. In mid-2005, the leading UK mapping website at that time, MultiMap had 7.3 million visitors and 47 million visitors used the leading USA equivalent, MapQuest.[10] In 2007, following the introduction into the market by Google, an estimated

[1] Dawn Kawamoto, *Internet Users Worldwide Surpass 1 Billion*, CNET NEWS, Jan. 23, 2009, http://news.cnet.com/8301-1023_3-10149534-93.html.

[2] *See generally* ORG. FOR ECON. CO-OPERATION AND DEV., BROADBAND GROWTH AND POLICIES IN OECD COUNTRIES (2008), *available at* http://www.oecd.org/dataoecd/32/57/40629067.pdf (examining broadband development and remaining policy challenges).

[3] *E.g.* Tim O'Reilly, *What Is Web 2.0*, O'REILLY, Sept. 30, 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

[4] *See* ORG. FOR ECON. CO-OPERATION AND DEV., PARTICIPATIVE WEB AND USER-CREATED CONTENT: WEB 2.0, WIKIS AND SOCIAL NETWORKING 53–66 (2007), *available at* http://213.253.134.43/oecd/pdfs/browseit/9307031E.PDF [hereinafter PARTICIPATIVE WEB] (describing growth of "user-created content" from technological developments and analyzing economic and social impacts).

[5] Adam Ostrow, *How Facebook Serves Up Its 15 Billion Photos*, MASHABLE, Apr. 30, 2009, http://mashable.com/2009/04/30/facebook-photo-sharing/.

[6] *Id.*

[7] *See* Arno Scharl, *Towards the Geospatial Web: Media Platforms for Managing Geotagged Knowledge Repositories*, *in* THE GEOSPATIAL WEB: HOW GEOBROWSERS, SOCIAL SOFTWARE AND THE WEB 2.0 ARE SHAPING THE NETWORK SOCIETY 4 (Arno Scharl & Klaus Tochtermann eds., Springer 2007) (describing geobrowsers as an interface metaphor for the Earth providing users with an accurate visual representation that lets them browse geospatial data from a satellite perspective).

[8] *See, e.g.*, Google Maps Mania, http://googlemapsmania.blogspot.com/ (last visited Feb. 23, 2010) (detailing thousands of different geo-mashups); Programmable Web, Mapping Mashups http://www.programmableweb.com/tag/mapping (last visited Feb. 23, 2010) (listing of various geo-mashups).

[9] *See* ELIZABETH GOODMAN & ANDREA MOED, COMMUNITY IN MASHUPS: THE CASE OF PERSONAL GEODATA 1 (2006), http://mashworks.net/images/5/59/Goodman_Moed_2006.pdf (defining geo-mashups as "hybrid sites that draw on freely available online map functionality").

[10] *See* Muki Haklay et al., *Web Mapping 2.0: The Neogeography of the GeoWeb*, 2 GEOGRAPHY COMPASS 2011 (2008) (providing an overview of geo-mashup development during the last fifteen years).

71.5 million users visited Google Maps and a further 22.7 million used Google Earth.[11] From 2005 to 2007 an estimated 50,000 mashups utilizing Google Maps were created.[12]

The rapid growth of geo-mashups highlights the shift from one-directional information provision in Web 1.0 to the bi-directional collaboration and interaction of Web 2.0.[13] This change has brought with it a concomitant set of new privacy concerns. Zittrain categorizes these new privacy problems as Privacy 2.0 and provides a cogent argument for the application of new ways to think about privacy in "the generative Internet."[14] He argues that innovative applications of privacy protection are required that transcend the first generation of privacy laws which focus explicitly on information privacy and the regulation of organizational activities related to the collection, storage, and use of personal information.[15] First generation limits arise in Web 2.0 structures because new data relationships emerge from the active participation of individual Internet users as well as governmental or corporate bodies. Using Zittrain's work,[16] the author contends that threats arising from privacy invasive geo-mashups require the implantation of effective protections in the fabric of technical and social structures that surpass the legislative limits and the regulatory capabilities of first generation laws.

Part II highlights Web 2.0 growth and the rise of geo-mashups. Two types of geo-mashups are identified: location and function oriented. Part III identifies a small number of privacy invasive geo-mashups that have given rise, or have the potential to give rise, to privacy concerns. Part IV details Zittrain's Privacy 2.0 and examines his criticism of first generation information privacy laws in light of changing information relationships. Part V, applies

[11] *See* Mark Sweney & Jemima Kiss, *Microsoft Buys Multimap*, GUARDIAN, Dec. 12, 2007, http://www.guardian.co.uk/media/2007/dec/12/microsoft.digitalmedia/print (providing usage statistics for Google Maps, Google Earth, Microsoft Windows Live Maps, and Multimap).

[12] Posting of Thai Tran to Google Lat Long Blog, http://google-latlong.blogspot.com/2007/07/google-maps-mashups-20.html (July 11, 2007, 5:58 EST).

[13] *See* Michael F. Goodchild, *Citizens as Sensors: The World of Volunteered Geography*, 69 GEOJOURNAL, 211, 214–215 (2007) [hereinafter Goodchild, *Citizens as Sensors*] (describing the movement from early web sites to Web 2.0 sites, which contain user-generated content and can be edited by users); Michael F. Goodchild, *Citizens as Voluntary Sensors: Spatial Data Infrastructure in the World of Web 2.0*, 2 INT'L J. OF SPATIAL DATA INFRASTRUCTURES RES. 24, 27 (2007) [hereinafter Goodchild, *Voluntary Sensors*] (explaining the difference between the early one-directional Web and the new bi-directional Web 2.0).

[14] *See* Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1975, 1981 (2006) [hereinafter Zittrain, *The Generative Internet*] (regarding the concept of generativity which "is a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility").

[15] *Id.* at 2018–20.

[16] In his work, Zittrain uses generativity as a concept that is wider than Web 2.0. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 123 (2008) (defining "Web 2.0" as "a new buzzword that celebrates this migration of applications traditionally found on the Internet to the PC. Confusingly, this term also refers to the separate phenomenon of increased user-generated content and indices on the Web – such as relying on user-provided tags to label photographs") [HEREINAFTER ZITTRAIN, THE FUTURE]. The author acknowledges the differences between Zittrain's concept of the generative Internet and the definition of Web 2.0 used in this Article. Nonetheless, the author contends that the interchangeable focus in this Article regarding Web 2.0 and the generative Internet is possible in the context of privacy invasive geo-mashups. That is because both concepts stress the importance of new information flows that highlight the limitations of first generation privacy laws.

key principles of Privacy 2.0 to a privacy invasive geo-mashup to highlight the limits of first generation information privacy laws. Part VI recommends Privacy 2.0 based technical and social solutions to mitigate the negative effects of privacy invasive geo-mashups. Finally, in Part VII, the author concludes by calling for the development of Privacy Standards for geo-mashups that would balance the requirements of continued geo-mashup innovation with the advancement of effective privacy protections against privacy invasive geo-mashups. These standards could assist the courts and privacy regulators regarding the interpretation of privacy laws in context with geo-mashups and thus aid the identification of privacy invasive geo-mashups.

II. WEB 2.0 AND GEO-MASHUPS

A brainstorming session at the Medialive International Conference in 2005 provided the first definition of the term "Web 2.0". The purpose of the conference was to identify the common effects of technologies that survived and flourished the 'dot.com' crash of the late 1990's.[17] The conceptual basis of the phenomenon that Web 2.0 describes varies,[18] but for the purposes of this paper it is defined as

> "a set of social, economic and technology trends that collectively form the basis for the next generation of the Internet—a more mature, distinct medium characterized by user participation, openness, and network effects."[19]

The key ideals of Web 2.0 reflect the use of the Internet to foster greater user participation, to increase openness, and to enhance sharing through a more decentralized structure.[20] The effect of Web 2.0 has been manifold in terms of technological, economic, and social developments.[21] Regarding technology, Web 2.0 has been a transformative impetus for the expansion of new technologies that concentrate on the delivery of information based online services to individual or collective Internet users rather than the provision of software to individual computer users.[22] For example, the makers of high

[17] *E.g.* Tim O'Reilly, *What Is Web 2.0*, O'REILLY, Sept. 30, 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

[18] *See, e.g.,* PARTICIPATIVE WEB, *supra* note 4, at 17 (defining the "participative web" which is intended to describe "the more extensive use of the Internet's capabilities to expand creativity and communication"); YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 30 (2006) (detailing the "networked information economy" which presents "the first modern communications medium that expands its reach by decentralizing the capital structure of production and distribution of information, culture, and knowledge"); ZITTRAIN, *The Generative Internet, supra* note 14, at 1981 (defining the "generative Internet").

[19] *See* JOHN MUSSER & TIM O'REILLY, WEB 2.0 PRINCIPLES AND BEST PRACTICES 12 (2007).

[20] *See* BENKLER, *supra* note 18, at 3 (explaining the difference between the networked information economy and the displaced industrial information economy).

[21] *See* PARTICIPATIVE WEB *supra* note 4, at 27 ("There [is] a range of technological, social, economic and institutional drivers of user-created content accounting for its rapid growth and pervasiveness.").

[22] *See, e.g.,* Lisa Veasman, "*Piggy Backing" on the Web 2.0 Internet: Copyright Liability and Web 2.0 Mashups*, 30 HASTINGS COMM. & ENT. L.J. 311, 313–17 (2008) (highlighting the types of technologies used in Web 2.0 and differences from the previous Internet era).

quality word processing software geared their products towards individual personal computers and governed software use through specific license agreements. Now, such software is freely available over the Internet.[23] In economic terms, shifting technology patterns fostered a change in how online technology providers perceived Internet users. Companies realized that greater user involvement through active participation in product development, adds value to the enduring expansion of "perpetual beta technologies".[24] Internet users were not just content consumers, but they were now content producers.[25] Online software companies tailored designs to match Internet user needs through new information exchange channels that led to the greater sharing of knowledge.[26] Successful Web 2.0 companies exploited the collective intelligence of Web communities through customer interaction and facilitated collaboration with Internet users.[27]

The change of Internet users from passive content consumers to active co-producers heralds the most significant social modification caused by Web 2.0.[28] New technologies provided a foundation for the rapid escalation in the amount of user generated content published online.[29] New modes of online service delivery enabled the collection and publication of information from mobile devices that made Internet user participation more relevant and instantaneous.[30] The use of everyday consumer devices, such as digital cameras and mobile phones, as mobile information collectors, enabled the incorporation of geographical elements with the publication of user generated content.[31] For the first time, it was easy to combine and share disparate sets of

[23] *See, e.g.*, Edward Lee, *Warming up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1500–01 (2008) (regarding the transfer of traditional desktop to web-based applications).

[24] *See* MUSSER & O'REILLY *supra* note 19, at 5–8, 15 (describing the development process, involving sampling, testing and actively responding to user activity and feedback to decide if development objectives are being met).

[25] *See* AXEL BRUNS, BLOGS, WIKIPEDIA, SECOND LIFE, AND BEYOND: FROM PRODUCTION TO PRODUSAGE 34 (2008) (defining a content producing Internet user as a "produser" to describe the idea of an Internet users as both a producer and user of technologies and information).

[26] *See* ZITTRAIN, THE FUTURE, *supra* note 16, at 84 ("[g]enerative systems allow users at large to try their hands at implementing and distributing new uses").

[27] *See* Mohamed Bishr & Lefteris Mantelas, *A Trust and Reputation Model for Filtering and Classifying Knowledge About Urban Growth*, 72 GEOJOURNAL 229, 235–36 (2008) (regarding the provision of geospatial related information in Web 2.0).

[28] *See* Lee, *supra* note 23, at 1504 (describing consumer transition from "couch-potato" to "active participants in the creation of expressive works" as a social good, in that it reaches new audiences and epitomizes the freedoms of the First Amendment).

[29] *See id.* at 1501 (regarding the growth of user generated content generated by the power of the Internet and its various "social networking platforms").

[30] *See, e.g.* Scharl, *supra* note 7, at 5 (noting the various images, including maps, that can be projected through the service by users' "GPS-enabled handsets"); *see also* David Tulloch, *Many, Many Maps: Empowerment and Online Participatory Mapping*, 12 FIRST MONDAY (2007), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/224 (regarding the use of new Internet mapping tools that "are creating a newly empowered class of users").

[31] *See* Claus Rinner, et al., *The Use of Web 2.0 Concepts to Support Deliberation in Spatial Decision-Making*, 32 COMPUTERS, ENV'T & URB. SYS. 386, 387 (2008) (highlighting the natural geospatial element to much user generated material "which increasingly is made explicit by adding geographic coordinates to the material's metadata (i.e. geotagging it). This way, the content can be visualized on a map and in some cases, the map material itself is user-generated content.").

information, related to specific geographical locations, with other users via publication on the Internet.[32] The sharing of user geographical information spawned a user-based, geo-mashup cottage industry fueled by the arrival of user-friendly, online mapping interfaces that facilitated the production of geo-mashups.

Free and easy-to-use geo-browsers such as Google Maps,[33] and to a lesser extent, Yahoo Maps,[34] Microsoft Live Maps[35] and NASA's Worldwind[36] provide a platform for non-technical users to overlay information on mapping interfaces to create geo-mashups.[37] The geo-browsers present a geospatial and visual representation of the world that is accessible via the Internet to integrate different types of data with specific geographical locations. In terms of geo-mashup technical development, application programming interfaces (APIs) have been the key enhancement.[38]

APIs are largely responsible for the growing popularity of mashups as they are able to combine different sources of publicly available data and provide an interface, either free or for a cost recovery charge, for different services based on data supplied by multiple providers.[39] As regards geo-mashups, APIs have facilitated third party online services by making the aggregation of different sets of information easier and have made the publication of overlays onto geo-browsers a relatively simple matter.[40] Because they "are relatively easy to use, APIs have made application development more accessible" and have enabled a wider community of Internet users to create, share and publish geographic information.[41] Internet

[32] *See* Kei-Hoi Cheung, et al., *Semantic Mashup of Biomedical Data*, 41 J. BIOMED. INFO. 683, 683, 685 (2008) (describing mashup tools that allow end-users to manipulate and publish their data on various web sites in the form of photos and maps).

[33] Google, Google Maps, http://maps.google.com/ (last visited Feb. 17, 2010).

[34] Yahoo!, Yahoo Maps, http://maps.yahoo.com/ (last visited Feb. 17, 2010).

[35] Microsoft, Live Search Maps, http://maps.live.com/ (last visited Feb. 17, 2010).

[36] NASA, Worldwind, http://worldwind.arc.nasa.gov/index.html (last visited Feb. 17, 2010).

[37] *See* Scharl, *supra* note 7, at 5 (explaining how geo-browers and other platforms, such as Sigalert.com and Google Earth, aggregate traffic and accident data from users and project it onto a map).

[38] MARTIN C. BROWN & CORPORATION EBOOKS, HACKING GOOGLE MAPS AND GOOGLE EARTH (2006); *See* VLAD TANASESCU, ET AL., THE GEOSPATIAL WEB: HOW GEOBROWSERS, SOCIAL SOFTWARE AND THE WEB 2.0 ARE SHAPING THE NETWORK SOCIETY 247 (2007) (regarding the distribution of APIs, such as Google Maps, and the resulting growth of geo-mashups due to Web 2.0 maps and their "map reality effect"). *See generally* ANDREW J TURNER, INTRODUCTION TO NEOGEOGRAPHY (2006).

[39] Posting of Brady Forrest to O'Reilly Radar, http://radar.oreilly.com/2009/05/google-launches-maps-data-api.html (May 20, 2009) (regarding how Google could become a geodata supplier as well as a mapping interface provider); *see* Google Code, Google Maps Data API, http://code.google.com/apis/maps/documentation/mapsdata/ (last visited Oct. 24, 2009) (regarding the announcement of a new API that allows "client applications to view, store and update map data in the form of Google Data API feeds using a data model of *features* (placemarks, lines and shapes) and *maps* (collections of features)"); *see also* ZITTRAIN, THE FUTURE, *supra* note 16, at 124 (regarding the generative effects of the Google Maps API).

[40] *See* Scharl, *supra* note 7, at 5 ("Most providers of geobrowsing platforms offer *Application Programming Interfaces (APIs)* or *XML scripting* to facilitate building third-party online services on top of their platforms (Roush 2005).").

[41] *See* Haklay et al., *supra* note 10, at 2020 (noting the "simpler tools [for geomashing] that, when deployed, enable a more pleasurable and effective user experience").

users could now easily aggregate cartographic data with geo-tagged,[42] individual user knowledge, such as a photo of a certain place or an advert for a business.[43] For example, software engineer Paul Rademacher created HousingMaps.com,[44] one of the first web mashups,[45] in 2005, when he aggregated a list of San Francisco real estate properties for sale, from the Craigslist website, with Google Maps, using residential address information as the aggregation point for the map overlay.[46] In the same year, Scipionus.com[47] highlighted the potential social benefits of geo-mashups following the aftermath of Hurricanes Katrina, Rita, and Wilma in New Orleans, Louisiana and Florida respectively.[48] Scipionus.com produced an interactive map of the disasters, populated by Internet users on the ground, which provided helpful and important information to other Internet users and for government authorities involved in rescue and relief.[49] Internet users added notes to locations on Google Maps that enabled residents of affected areas to enquire and receive information about missing persons and about the status of their homes and communities.[50]

Whilst the use of APIs have enhanced the interoperability of different data sets, the other key factor in the growth of geo-mashups has been the greater availability of information in forms that can be readily used for geospatial aggregation purposes.[51] One of the key social effects of the previous decade has been the wider availability of geographic and statistical information, and more importantly, the greater willingness of organizations to share their data, either free, or for fees that enable and encourage innovation.[52] As highlighted above, Internet users have also been more willing to share their

[42] *See* Scharl, *supra* note 7, at 5 (defining geotagging as the "process of assigning geospatial context information, ranging from specific point locations to arbitrarily shaped regions").

[43] Rinner et al., *supra* note 31, at 386.

[44] HousingMaps, http://www.housingmaps.com/ (last visited Feb. 21, 2010).

[45] *See* MUSSER & O'REILLY, *supra* note 19, at 28.

[46] *Id.*

[47] The Scipionus website is no longer available on the Internet.

[48] *See* Official Google Australia Blog: Mapping the Victorian Fires, http://google-au.blogspot.com/2009/02/mapping-victorian-fires.html (last visited Feb. 21, 2010) (regarding a geo-mashup similar in principle to Scipionus developed by Google regarding the Victorian Bushfire disaster in February 2009 to provide assistance and information to people affected by the fires and emergency services personnel).

[49] *See* Christopher C. Miller, *A Beast in the Field: The Google Maps Mashup as GIS/2*, 41 CARTOGRAPHICA 187, 194–95 (2006) (regarding further details about the Scipionus website).

[50] Jacqueline W. Mills & Andrew Curtis, *Geospatial Approaches for Disease Risk Communication in Marginalized Communities*, 2 PROGRESS IN COMMUNITY HEALTH PARTNERSHIPS: RESEARCH, EDUCATION, AND ACTION, 61, 68–69 (2008).

[51] *See* Marin Perez, *Nokia Enters Google Territory, Opens up Mapping API,* INFORMATION WEEK, May 20, 2009 http://www.informationweek.com/news/software/development/showArticle.jhtml?articleID=217600266&subSection=All+Stories (regarding Nokia's new API for Ovi Maps which is claimed to be "the first step toward an ecosystem where developers can access Nokia's unique contextual assets, such as location, to create mobile applications that will redefine how we use our mobile devices" (quoting Michael Halbherr, VP of Nokia's social location services)).

[52] *See* John Palfrey & Urs Gasser, *Case Study: Mashups Interoperability and eInnovation 3* (The Berkman Ctr. for Internet & Soc'y at Harv. L. Sch., Nov. 2007), http://cyber.law.harvard.edu/interop/pdfs/interop-mashups.pdf (stating that two ingredients of mashups are the data and application programming interfaces, which provide access to "malleable" forms of data for non-programmers).

information with other users for geo-mashup purposes.[53]

User provided information for mapping purposes has been categorized as volunteered geographic information (VGI)[54] and is seen as part of the wider ambit of Neogeography[55] or GIS/2.[56] Technologies, such as Global Positioning Systems (GPS) and Radio Frequency Identification (RFID), in widespread consumer devices such as mobile phones, palmtops, satellite navigation systems and digital cameras has made the proliferation of VGI possible. It is now possible for an Internet user to plot their destination in line with the use of their consumer goods.[57] For example, digital cameras or mobile phones with inbuilt GPS can automatically provide a latitude and longitude reading for any photograph taken on the device.[58] Not only has this enhanced a user's ability to record a wealth of new geographically related information, but it has also had the effect of making human beings geographical sensors.[59] For example, geo-mashups now exist for cyclists to share information about cycle routes,[60] for runners to plan details of running routes[61] and for anglers to reveal the sites of secret fishing holes.[62]

These geo-mashups are defined as location oriented geo-mashups because

[53] *See* Miller, *supra* note 49, at 192 (explaining the relationship between the increase of user generated content and Google Maps).

[54] *Compare, e.g.*, Goodchild, *Citizens as Sensors*, *supra* note 13, at 217–20 (regarding VGI), *and* Bishr & Mantelas, *supra* note 27, at 229–30 (regarding the concept of Collaboratively Contributed Geographic Information (CCGI)), *with* Andrew Flanagin & Miriam Metzger, *The Credibility of Volunteered Geographic Information*, 72 GEOJOURNAL 137, 142 (2008) (regarding a critical examination of the credibility of VGI), *and* ANDREW KEEN, THE CULT OF THE AMATEUR 64–68 (2007) (regarding more general concerns about the accuracy of information collected and published on the Internet).

[55] *See, e.g.*, TURNER, *supra* note 38, at 3 (defining Neogeography as "people using and creating their own maps, on their own terms and by combining elements of an existing toolset"); Haklay, et al., *supra* note 10, at 2021 (contrasting the difference between traditional cartographic sciences and Neogeography).

[56] *See, e.g.*, Miller, *supra* note 49, at 189 (describing GIS/2 as "a proposed alternative to mainstream GIS that would account for the less rigid, more socially and culturally mutable information needs of user groups being shut out by GIS/1.").

[57] *See* Goodchild, *Citizens as Sensors*, *supra* note 13, at 212 (highlighting GPS enabled mobile phones and digital cameras are able to take photos with automatic metadata tags of latitude and longitude readings of the photograph location); Scott Counts & Marc Smith, *Where Were We: Communities for Sharing Space-Time Trails*, *in* PROCEEDINGS OF THE 15TH ANN. ACM INT'L SYMPOSIUM. ON ADVANCES IN GEOGRAPHIC INFO. SYS. (Hanan Samet et. al., ed. 2007), http://doi.acm.org/10.1145/1341012.1341026 (regarding a typography of such technologies); Official Google Mobile Blog: Your Maps in Your Hands for the Holidays, http://googlemobile.blogspot.com/2008/12/your-maps-in-your-hands-for-holidays.html (Dec. 15, 2008, 11:07 EST) (regarding the next stage of development relating to Google Android and the recording of geospatial data that will allow users to "create, edit, share, and view personalized maps on your Android powered phone synchronized with the My Maps tab on Google Maps. . . .Your maps are automatically synchronized with your My Maps on the web").

[58] Goodchild, *Citizens as Sensors*, *supra* note 13, at 212.

[59] *See* Goodchild, *Voluntary Sensors*, *supra* note 13, at 25–27 (explaining that humanity as a whole has a wealth of geographic knowledge that is only enhanced through the use of technology).

[60] Reid Priedhorsky, et al., *How a Personalized Geowiki Can Help Bicyclists Share Information More Effectively*, *in* PROCEEDINGS OF THE 2007 INT'L SYMPOSIUM. ON WIKIS 93–98 (2007), *available at* http://doi.acm.org/10.1145/1296951.1296962; Reid Priedhorsky & Loren Terveen, *The Computational Geowiki: What, Why, and How*, *in* PROCEEDINGS OF ACM CSCW'08 CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK 267–276 (2008), *available at* http://doi.acm.org/10.1145/1460563.1460606.

[61] Mapmyrun.com, http://www.mapmyrun.com/ (last visited Nov. 18, 2009).

[62] Fishing Lake Map, 1001 Secret Lake Fishing Maps!, http://www.1001seafoods.com/fishing/fishing-maps.php (last visited Nov. 18, 2009).

they allow users to provide or upload information relating to a specific geographical location. Other geo-mashups that fall within this category include Wikimapia.com[63] that provides a vetted service where users can provide descriptions of places of interest along with geographic coordinates, as long as the comments meet specified criteria[64] and Flickr, the photography-publishing website that allows users to geotag uploaded photos to a specific location.[65] Furthermore, Platial.com, is a social networking site where users can provide comments or maps related to geographic points or their experiences around specific geographic points[66] and Placeopedia.com overlays information published on Wikipedia over a geographic location. [67] Finally, OpenStreetMap[68] is an open access street map of the world in which users populate information about specific locations.

Another type is function-oriented geo-mashups. These geo-mashups overlay information with a mapping interface to provide a geographical context related to a specific publication purpose. For example, the London Profiler[69] geo-mashup provides a range of statistical and public data on London boroughs and Who Is Sick?[70] provides user generated information about illnesses contracted by individuals in geographical areas. Furthermore, the Tunisian Prison Map[71] geo-mashup provides the location of prisons in Tunisia and details human rights violations of prisoners held within those prisons and Topobiographies of the Catalan Exile[72] tracks exiles who fled from Spain during the Spanish Civil War. The One Big Thing[73] geo-mashup provides information on the US Federal Government's stimulation package spending and Antenna Search[74] provides the location of mobile phone antenna masts anywhere in the USA. Finally, the Hospital Rankings[75] geo-mashup provides quality assurance information of US hospitals based on type of illness.

The author contends that function oriented geo-mashups can particularly give rise to privacy concerns because of how they use both personal and non-personal information with a residential address, as shown in the next part of the article.

[63] Wikimapia—Let's Describe the Whole World!, http://wikimapia.org/ (last visited Nov. 18, 2009).

[64] *See* Goodchild, *Voluntary Sensors*, *supra* note 13, at 28 (explaining Wikimapia).

[65] About Flickr, http://www.flickr.com/about (last visited May 19, 2009).

[66] Platial.com—Who and What's Nearby, About Us, http://platial.com/about (last visited May 19, 2009).

[67] Placeopedia, http://www.placeopedia.com/ (last visited May 19, 2009).

[68] OpenStreetMap, http://www.openstreetmap.org/ (last visited May 31, 2009).

[69] London Profiler, http://www.londonprofiler.org/ (last visited May 19, 2009).

[70] Who Is Sick?, http://whoissick.org/sickness/ (last visited May 19, 2009).

[71] Tunisian Prison Map, http://www.kitab.nl/tunisianprisonersmap/ (last visited May 19, 2009)

[72] Universitat Oberta De Catalunya, Topobiographies of the Catalan Exile, http://www.topobiografies.cat/en/ (last visited Feb. 20, 2010).

[73] David Erickson, The One Big Thing: Federal Government Spending Data Mashups, http://e-strategyblog.com/2009/04/the-one-big-thing-federal-government-spending-data-mashups/ (last visited Feb. 20, 2010).

[74] Antenna Search, http://www.antennasearch.com/ (last visited Feb. 20, 2010).

[75] Netdoc.com, Hospital Rankings, http://www.netdoc.com/hospital-rankings (last visited Feb. 20, 2010).

III. PRIVACY-INVASIVE GEO-MASHUPS

A small number of geo-mashups have created, or have the potential to create, privacy concerns that involve the unauthorized use of personal information, the inadvertent disclosure of personal information and invasion of privacy issues. Geo-mashups that give rise to privacy issues are labeled privacy invasive geo-mashups because they able to intrude into an individual's privacy.[76] The definition of a privacy invasive geo-mashup is intentionally broad to transcend privacy issues based solely on personal information use. As Solove comments, a conception of privacy based purely on control over information only partially captures the problems that arise from increased use of personal information.[77] For the sake of completeness, privacy protection is defined as the "process of finding appropriate balances between privacy and multiple competing interests".[78] That said, however, as this article is an introduction to the concept of privacy invasive geo-mashups and the limits of first generation information privacy laws, the author concentrates mostly on issues that arise from the use and re-use of personal information.

It is also important to concede that the small number of privacy invasive geo-mashups detailed is a minuscule fraction of the total number of geo-mashups currently published on the Internet. Whilst the examples may not be representative of the total geo-mashup population, they nonetheless provide clear indications of the types of problems that can emerge and emphasize the capacity privacy invasive geo-mashups have to affect a large number of individuals,[79] as evidenced by the first example.

A. Unauthorized Use of Personal Information

In this sub-section, two geo-mashup examples are used to demonstrate concerns involving the unauthorized publication of personal information. The first gave rise to actual privacy problems whereas the second could have

[76] *See* Roger Clarke, Introducing Pits and Pets: Technologies Affecting Privacy, http://www.rogerclarke.com/DV/PITsPETs.html#Terms (last visited Feb. 20, 2010) (regarding the article's definition of privacy invasive geo-mashups which is based on Clarke's definition of privacy invasive technologies).

[77] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1154 (2002). *See* Anita L. Allen, *Privacy as Data Control: Conceptual, Practical and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 869 (2000) (regarding the conceptual and practical limits of information privacy as control over personal information "privacy is open to broader and more perspicacious definitional analysis. . . . It is pointless (or merely symbolic) to ascribe a right to data control if it turns out that exercising the right is impossible"); Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 127 (2003) (regarding the difficulty in distinguishing specific normative arguments about privacy as control against more general principles of liberty and autonomy).

[78] Roger Clarke, Privacy: More Wobble-Board Than Balance-Beam, http://www.rogerclarke.com/DV/Wobble.html (last visited Feb. 20, 2010).

[79] The author acknowledges the social benefits that can arise from geo-mashups and this article should not be viewed as a general criticism of the use of geo-mashups or a call to restrict geo-mashup innovations. Geo-mashups provide exciting and new opportunities to involve members of the public and thus creates greater awareness to geographic, cartographic and indeed broader social issues. However, the author contends that the privacy issues raised from privacy invasive geo-mashups need to be addressed and discussed further.

caused privacy concerns if published. The first example entails the membership list of the British National Party and gives rise to serious privacy concerns as identified in later parts of this article.

1. *British National Party Membership List*

The British National Party[80] (BNP) is a nationalist political party based in the United Kingdom.[81] The BNP contends that it is a legitimate democratic organization despite its historical background, which has links to racially related and politically motivated violence and involvement with far-right paramilitary groups, both in the UK and overseas.[82] Despite attempts at political legitimization, BNP policies remain fervently right wing.[83] Rank-and-file membership of the BNP is therefore a sensitive issue especially as some professions preclude membership of the party[84].

On November 18 2008, a disgruntled former BNP employee published the 12,000 plus party membership list on the Internet.[85] Previously, five individuals acquired the membership list without authorization in April 2008. The BNP obtained an injunction against them, which prohibited the publication

[80] The author has no political allegiances with the BNP and this example is used solely to highlight the privacy issues that can emerge from privacy invasive geo-mashups. Moreover, the author respects the right of individuals to keep their political allegiances private should they choose to do so.

[81] British National Party, http://bnp.org.uk/ (last visited Feb. 20, 2010).

[82] *See* Wikipedia, British National Party, http://en.wikipedia.org/wiki/British_National_Party (last visited Feb. 20, 2010) (providing a concise history of the BNP).

[83] *E.g.* BNP, Immigration, http://bnp.org.uk/policies/immigration/ (last visited Feb. 20, 2010) ("We will abolish the 'positive discrimination' schemes that have made white Britons second-class citizens. We will also clamp down on the flood of 'asylum seekers', all of whom are either bogus or can find refuge much nearer their home countries").

[84] *E.g.* ACPO Bans Police from Joining BNP, BBC NEWS, July 27, 2004, http://news.bbc.co.uk/2/hi/uk_news/3930175.stm (regarding the Association of Chief Police Officers (ACPO) ban on membership of the BNP in UK police forces); Christopher Hope, *How Many BNP Activists Live in Your Town? Now You Can Find Out*, THE TIMES, Nov. 20 2008, http://www.telegraph.co.uk/news/newstopics/politics/3484489/How-many-BNP-activists-live-in-your-town-Now-you-can-find-out.html ("There is no question that the BNP is widely viewed with deep suspicion. Police officers, for example, cannot join because it "would be incompatible with our duty to promote equality under the Race Relations Amendment Act and would damage the confidence of minority communities" (quoting Greater Manchester Police Chief Constable, Peter Fahy)).

[85] BNP Activists' Details Published, BBC NEWS, Nov. 18, 2008, http://news.bbc.co.uk/2/hi/uk_news/7736405.stm; Esther Addley & Haroon Siddique, *BNP Membership List Posted Online by Former 'Hardliner'*, THE GUARDIAN, Nov. 19 2008, http://www.guardian.co.uk/politics/2008/nov/19/bnp-list; Dominic Kennedy & Nico Hines, *Thousands in Fear after BNP Members List Leak*, THE TIMES, Nov. 19 2008, http://www.timesonline.co.uk/tol/news/politics/article5183833.ece; James Kirkup & Christopher Hope, *BNP Membership List Leaked onto Internet*, THE DAILY TELEGRAPH, Nov. 19 2008, http://www.telegraph.co.uk/news/newstopics/politics/3479612/BNP-membership-list-leaked-onto-internet.html (describing the contents of the members list); Ben Russell, *BNP Membership List Published on Internet*, THE INDEPENDENT, Nov. 19 2008, http://www.independent.co.uk/news/uk/politics/bnp-membership-list-published-on-internet-1024719.html (detailing the publication of home addresses, phone numbers and emails of about 13,500 people on the BNP members list); James Sturcke et al., *BNP Membership List Leaked Online*, THE GUARDIAN, Nov. 18 2008, http://www.guardian.co.uk/politics/2008/nov/18/bnp-membership-list-leak (informing the public about the publication of the list).

of the list and ordered the destruction of any copies.[86] The membership list was nonetheless disseminated in November 2008 and published details included names, addresses, telephone numbers, email addresses and in some cases, employment details. The list also included the names and ages of children who have become members of the party after a parent had taken out a family membership, and several people who have joined the party at the age of 16.[87] Moreover, the BNP admitted that the list was only partially correct as it included the names of persons who had never been party members.[88] Media sources reported that Dyfed Powys Police arrested and charged two persons with criminal offences under the Data Protection Act 1998, in a joint investigation with the Information Commissioner's Office, regarding the publication of the list.[89]

Wikileaks, [90] a website that provides online space for the publication of anonymous submissions of sensitive corporate or government material published the membership list on the Internet. Different organizations and individuals used Bit Torrent and social networking websites[91] to copy and disseminate the list further. More importantly, in terms of this article, both media organizations and individuals used the membership list to create geo-mashups based on its content. For example, the Times provided an overlay of the BNP membership list on Google Maps to highlight postcode areas where BNP membership was at its highest.[92] Bubbles represented different postcode districts and different colored bubbles represented the density of BNP

[86] *See BNP Protest after Arrests*, MANCHESTER EVENING NEWS, Nov. 19, 2008, *available at* http://www.manchestereveningnews.co.uk/news/s/1080665_bnp_protest_after_arrests (explaining that BNP brought an injunction at the High Court in Manchester against five people to stop them publishing a list of party members).

[87] *See* Addley & Siddique, *supra* note 85 (describing the content of the list of members).

[88] *See id*. (describing the content of the list of members); Kirkup & Hope, *supra* note 83, at 5 (reporting that data collected and published on the list was of a rather unconventional nature: "[s]ome of the detail leaves the BNP open to mockery. Why, for example, would the BNP need to record the following about one member from Wiltshire: 'Hobbies: amateur radio & "church crawling". Quaker attender - proof of entitlement seen'? Or how about this, attached to the entry for one woman from the south of England: 'Owner of a WW2 jeep. Singer with a ladies' barber shop chorus and quartet'").

[89] *See BNP Expects More Arrests over Leaked Membership List*, NOTTINGHAM EVENING POST, Dec. 6, 2008, http://www.thisisnottingham.co.uk/crime/arrested-Notts-BNP-membership-leakarticle-527013-details/article.html (notifying about the arrests and describing the charges); *BNP List Arrest Pair Are Bailed*, BBC NEWS, Dec. 10, 2008, http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/7775631.stm 2009) (stating that the two arrested persons were bailed out); Ian Johnston, *Two Held over BNP Member List Leak*, THE INDEPENDENT Dec. 6, 2008, http://www.independent.co.uk/news/uk/home-news/two-held-over-bnp-member-list-leak-1054428.html (speaking about the arrests in Brinsley); Sarah Knapton, *Two Arrested over Leaking of BNP Membership List*, THE TELEGRAPH, Dec. 5, 2008, http://www.telegraph.co.uk/news/newstopics/politics/3568802/Two-arrested-over-leaking-of-BNP-membership-list.html; *Two Arrests over Leaked BNP List*, BBC NEWS, Dec. 5, 2008, http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/7768142.stm.

[90] Wikileaks, http://wikileaks.org (last visited Sept. 30, 2009).

[91] *See* Sam Leith, *What's 'Liberal' About Hacking into the BNP?*, THE TIMES, Nov. 22, 2008, http://www.telegraph.co.uk/comment/columnists/samleith/3563694/Whats-liberal-about-hacking-into-the-BNP.html (regarding publication of personal information from the BNP membership list on Facebook).

[92] BNP Membership by Postal District, THE TIMES, Nov. 19, 2008, http://www.timesonline.co.uk/tol/news/uk/article5191424.ece.

members in the postcode district.[93] The Guardian produced a similar geo-mashup showing the population density of BNP members by political constituency rather than postcode.[94]

Individual Internet users also created BNP geo-mashups. For instance, the "BNP Near Me" geo-mashup[95] initially used single red pinpoints to represent the location of BNP members by postcode. However, unlike the Times geo-mashup, the use of the red pinpoints gave a misleading impression as they inadvertently singled out an individual residential property on Google Maps even though the pinpoint represented a postcode district. The creator of the "BNP Near Me" subsequently altered the geo-mashup after he received voluble criticism about the apparent misrepresentation of postcode information.[96] Red heat spots, replaced the pinpoints, and provided a representation of postcode area without highlighting an individual property. Another BNP membership list geo-mashup is the "BNP Member Proximity Search".[97] An Internet user is required to enter a postcode into a search field and another webpage details those BNP members who reside within a two-mile radius of the entered postcode. Unlike the other BNP membership geo-mashups, the Proximity Search geo-mashup provides both postcode and name of BNP members. Additionally, another webpage, linked to the hyperlinked postcode, directs a user to Google Maps, which pinpoints a specific residential property.

The unauthorized release of the BNP membership list has had some serious consequences. Some BNP members have had their employment terminated[98] or have received death threats[99] and in one instance, a car

[93] *Id*.

[94] *BNP Members: The Far Right Map of Britain*, THE GUARDIAN, Nov. 19, 2008, http://www.guardian.co.uk/uk/interactive/2008/nov/19/bnp.

[95] Ben Charlton, *Leaked BNP Member List Map*, SPOD.CX, http://spod.cx/bnp_members_list.shtml (the original map has subsequently been removed and replaced).

[96] *See* Mike Butcher, *One More BNP Thing - Heatmaps Replace Pins, but Pandora's Box Is Now Open*, TECHCRUNCH EUROPE, Nov. 19, 2008, http://uk.techcrunch.com/2008/11/19/one-more-bnp-thing-heatmaps-replace-pins-but-pandoras-box-is-now-open/ (highlighting some of the consequences of the publication of the BNP list); Mike Butcher, *Updated: BNP Member List Mashed with Google Maps Creates a Sea of Red Dots, but Dangerously Inaccurate*, TECHCRUNCH EUROPE, Nov. 19, 2008, http://uk.techcrunch.com/2008/11/19/bnp-member-list-mashed-with-google-maps-creates-a-sea-of-red-dots/ [hereinafter Butcher, *Updated: BNP Member List*] (reporting potential inaccuracies and misrepresentations relating to the BNP Near Me geo-mashup).

[97] BNP Member Proximity Search, http://www.fishmech.net/bnp/ (last visited May 19, 2009).

[98] *See 'BNP Membership' Officer Sacked*, BBC NEWS, Mar. 21, 2009, http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/7956824.stm (regarding the sacking of a police officer for being a member of the BNP); *Church Asked to Ban BNP Members*, BBC NEWS, Jan. 19, 2009, http://news.bbc.co.uk/2/hi/uk_news/7838280.stm (highlighting that the Church of England Synod is considering banning clergy from joining the BNP after it was revealed that clergymen were members of the BNP); Joe Murphy, *Radio Host Exposed in BNP Leak is Axed*, LONDON EVENING STANDARD, Nov. 19, 2008, http://www.thisislondon.co.uk/standard/article-23589438details/Radio+host+exposed+in+BNP+leak+is+sacked/article.do (regarding the sacking of a national talk back radio presenter).

belonging to the neighbor of a BNP member was mistakenly petrol bombed.[100]

2. *Amazon.com's Wish Lists & Data Mining*

In January 2006, Tom Owad published an article on the Applefritter website about governmental use of data mining techniques.[101] Owad highlighted that large amounts of information can be easily data mined using readily available, home computer equipment. The purpose of his research was to highlight how much data mining the US Government could undertake with its much larger computing capabilities and information accessing powers. For instance, section 215 of the Patriot Act,[102] allows the Federal Bureau of Investigations ("FBI") to obtain a court order, without probable cause, from the Foreign Intelligence Surveillance Act Court regarding the production of "any tangible things (including books, record, papers, documents, and other items) for an authorized investigation to protect against terrorism or clandestine intelligence activities".[103] The legislation defines "any tangible thing" to include books withdrawn from a library.[104] In keeping with the nature and content of the Patriot Act, Owad conducted his experiment on wish lists created on the book-selling website Amazon.com.[105] Users can create an Amazon wish list as a guide for potential, future gift ideas[106] and by default, Amazon makes the wish lists public to anyone who conducts a search by name.[107]

It is also possible to send an item direct to the wish list creator if he or she has entered a shipping address. However, the downloadable wish lists only

[99] *BNP Members 'Targeted by Threats'*, BBC NEWS, Nov. 19, 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7736794.stm (regarding details of threats received by callers to a BBC radio program); *Death Threats as BNP Members Are Named*, THIS IS CORNWALL, Nov. 25, 2008, http://www.thisiscornwall.co.uk/northcornwall/Death-threats-BNP-members-named/article-499803-detail/article.html (regarding death threats to Cornish BNP members); *Death Threats for Politician after BNP Members List Is Leaked*, THE SENTINEL, Nov. 20, 2008, http://www.thisisstaffordshire.co.uk/news/Death-threats-follow-BNP-listarticle-488115-details/article.html (regarding death threats received by a BNP local councillor); Ian Watson, *Privacy Issues for BNP Members*, BBC NEWS, Nov. 19, 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7737651.stm (regarding the security of BNP members in Northern Ireland and the Irish Republic).

[100] *See* Nico Hines, *BNP Member Says Family Safety at Risk after Car Explodes Outside Home*, THE TIMES, Nov. 21, 2008, http://www.timesonline.co.uk/tol/news/uk/crime/article5204727.ece (explaining the car bombing outside a BNP member's home); *Police Probe BNP Link to Car Fire*, BBC NEWS, Nov. 21, 2008, http://news.bbc.co.uk/2/hi/uk_news/england/bradford/7741270.stm (discussing the firebombing of a BNP member's house).

[101] Posting of Tom Owad to Applefritter, Data Mining 101: Finding Subversives with Amazon Wishlists, http://www.applefritter.com/bannedbooks (Jan. 4, 2006, 19:37 EST).

[102] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107–156, 115 Stat. 272 (2001) [hereinafter Patriot Act].

[103] Patriot Act § 215.

[104] See Eric Lichtbau, *F.B.I., Using Patriot Act, Demands Library's Records,* N.Y. TIMES, Aug. 26 2005, http://www.nytimes.com/2005/08/26/politics/26patriot.html (regarding the first attempt by the FBI to use the powers under the Act to demand access to library records from a Connecticut institution).

[105] Amazon, http://www.amazon.com/ (last visited May 19, 2009).

[106] Amazon Wish List, http://www.amazon.com/gp/registry/wishlist/ (last visited May 19, 2009).

[107] Owad, *supra* note 101.

include city and state information and the full shipping address remains private.[108] Due to Amazon's popularity, a vast number of wish lists exist, and whilst it is not possible to search for a particular person in an index, it is possible to conduct a search by a particular forename, such as "Mark". Owad retrieved over 120,000 wish lists by using this type of search.[109] Owad then conducted a search on an unspecified, yet common, forename and downloaded 260,000 wish lists of US citizens. Owad selected some potentially subversive books and searched the wish list data to see who had chosen them.

The retrieved wish lists included forename but not street address. Owad was able to cross-reference the wish list names with Yahoo People Search[110] to obtain an address and telephone number of those people listed.[111] Owad then created a geo-mashup by overlaying the wish list information, with street addresses retrieved from Yahoo People Search over Google Maps. However, whilst the option was technically available to match an individual wish list entry by address to a specific satellite image of a home on Google Maps, Owad decided against this on the basis that it would be extreme and potentially lead to an invasion of an individual's privacy.[112] Instead, Owad used city names and states as the basis for geographical aggregation. The Amazon subversive book geo-mashup nonetheless shows the issues that can arise from the unauthorized aggregation of information with a residential address.

B. Inadvertent Disclosure of Personal & Sensitive Information

The following sub-section examines two geo-mashup examples featuring the inadvertent disclosure of personal or sensitive information. The first involves the publication of crime statistics and the use of Google Streetview and the second entails the use of Google's My Maps function to create and publish user generated geo-mashups.

1. Crime Maps

One of the first geo-mashup incarnations was the Chicago Crime Maps website,[113] which overlaid crime statistics and information from the Chicago Police Department over Google Maps. The resultant geo-mashup was seen as "a profoundly civic-minded utility: a light GIS built by a single citizen that takes one base map and a freely available store of data and makes meaning of the two in ways that can easily reach members of that community".[114]

The success of Chicago Crime Maps spawned a number of different crime related geo-mashups by law enforcement authorities and by individuals.

[108] *Id*.

[109] *Id*.

[110] Yahoo People Search, http://people.yahoo.com/(last visited May 19, 2009).

[111] Owad, *supra* note 101.

[112] *Id*.

[113] Everyblock Chicago, http://chicago.everyblock.com/crime/ (last visited May 19, 2009). The Chicago Crimes website was formerly known as chicagocrime.org and is represented as such in the older literature.

[114] Miller, *supra* note 49, at 192.

For example, the Los Angeles Police Department offers a crime map that provides up to date information on crimes in the city.[115] On a wider scale, Crime Reports[116] works with 468 different law enforcement agencies that provide the website with details of the latest crimes. Crime Reports then geocode the crime data and send email alerts to users who have requested updated information from a specific agency. Crime Reports then overlays crime data on a Google Map and pinpoints to a specific location.[117] However, Crime Reports protects the privacy of crime victims by ensuring that

> Law enforcement agencies remove victim identification as part of the data publishing process. In addition, we help protect victim identities by converting the exact street addresses to the "block level". For example, the address "1486 Lincoln Avenue" would be mapped and displayed as "1400 block of Lincoln Avenue".[118]

The Metropolitan Police's crime map of London also highlights the sensitivity inherent in the wider reporting of crime statistics.[119] Unlike their US counterparts, the Metropolitan Police will only release information of crimes at a borough or ward level rather than an individual street or location. Media organizations have also provided similar geo-mashups.[120] The LA Times Homicide Map[121] details every homicide in Los Angeles County. An Internet user can view murders committed in a particular location or can click on the name of a murder victim and a Google Map pinpoints the location of the crime. An Internet user can then click on the pinpoint tag for the crime, which is hyperlinked to the LA Times Blog, The Homicide Report for more details and user comments.[122] However, whilst Google Maps tags the pinpoint to a specific property, it is unclear whether this is the actual address of the crime or whether it is representative of a wider aggregation source, such as zip code.

Spotcrime[123] is similar in concept to the geo-mashups highlighted above. Like Crime Reports, the geo-mashup uses crime statistics but it also has an option for Internet users to provide details of certain crimes.[124] These crimes

[115] Los Angeles Police Department, Crime Maps, http://www.lapdcrimemaps.org/ (last visited May 20, 2009).

[116] Crime Reports, http://crimereports.com/lea/cr (last visited May 20, 2009).

[117] Crime Reports, How It Works, http://crimereports.com/lea/crhowitworks (last visited May 21, 2009).

[118] Crime Reports, FAQs, http://crimereports.com/company/faq#whycreated (last visited May 19, 2009).

[119] Metropolitan Police, Metropolitan Police Crime Mapping, http://maps.met.police.uk/ (last visited May 21, 2009).

[120] *See* Berliner Kurier, Berlin Crime Map, http://www.berliner-kurier.de/blaulichtkurier/ (last visited May 20, 2009) (showing the use of crime mapping in Germany as provided by a media group).

[121] Los Angeles Times, The Homicide Map, Los Angeles County Victims, http://www.latimes.com/news/local/crime/homicidemap/ (last visited May 20, 2009).

[122] *E.g. The Homicide Report*, L.A. TIMES, May 14, 2009, http://latimesblogs.latimes.com/homicidereport/2009/05/crenshaw-michael-mccullough-15.html#comments (regarding the murder of Michael McCullough).

[123] Spotcrime - Know Your Neighborhood, http://www.spotcrime.com/ (last visited May 21, 2009).

[124] *See* Spotcrime, Spotcrime Help, http://www.spotcrime.com/help.php (last visited May 21, 2009) (regarding a user's opportunity to report crimes relating to theft, burglary, robbery, assault, arson, shootings, vandalism and arrests).

are searchable on the SpotCrime website along with user-supplied information. SpotCrime acknowledges the sensitivity in the reporting of crimes by partially redacting address information.[125] An Internet user can click on a reported crime to open a new webpage, which supplies a zoomed in version of the geo-mashup that provides basic crime details, such as the type of crime, the case number and the partially redacted address. The webpage also activates Google Streetview[126] and it provides a ground level photo image of the geo-tagged residential property.

The use of Google Streetview can give rise to privacy concerns relating to sensitive crimes, particularly rape. A user cannot search for rape related crimes on SpotCrime because it is not one of the searchable categories.[127] It is unclear whether SpotCrime intends to report rape crimes because they are not categorized by their own searchable group. However, the author discovered one report of a rape crime in the Los Angeles area, which was classified as an 'assault' in SpotCrime, in which the street address was redacted but the street number was clearly visible on Google Streetview,[128] thus making the redaction of street address irrelevant. The residential property highlighted by Google Streetview is a small apartment block that appears to have a limited number of apartments, which could make it easier to identify the victim.

2. *Google's My Maps*

In November 2008, 37 schools in Japan inadvertently disclosed the personal information of 980 school students on Google Maps.[129] In Japan, it is customary for teachers to visit the homes of pupils who are about to start a new school.[130] Several teachers of primary and secondary school pupils used the My Maps[131] feature on Google Maps to ascertain directions and to record certain information about the pupils, such as name and telephone numbers.[132] The teachers' tagged residential addresses with information provided by the pupil and used My Maps as a convenient tool to find the quickest route from one pupil's house to another.[133] A vice principal of one of the schools in the affected areas stated that "[f]or teachers unfamiliar with local geography, it can

[125] Typically, the last two digits are replaced from a house address number with 'XX', for example "205XX Roscoe BL" or "7XX W 148th ST." It would appear that the Los Angeles Police Department conducts this process automatically. Spotcrime - Most Wanted – Most Viewed Crimes, http://www.spotcrime.com/mostviewed.php (last visited Feb. 19, 2009).

[126] Google, Google Maps Street View, http://maps.google.com/help/maps/streetview/faq.html (last visited Oct. 20, 2009).

[127] SpotCrime, *supra* note 125.

[128] The author does not intend to provide details of the incident for obvious reasons of sensitivity. However, SpotCrime has been informed about the situation.

[129] *Student Data Slip out via Google Maps*, YOMURI SHIMBUN, Nov. 18, 2008, http://educationinjapan.wordpress.com/edu-news/current-concerns-8/current-concerns-9/current-concerns-12-teachers-slip-up-via-google-map-use-school-stabbing-cannabis-crimes.

[130] *Id.*

[131] Google Lat Long Blog, Save and Share Directions with My Maps, http://google-latlong.blogspot.com/2009/04/save-and-share-directions-with-my-maps.html (last visited Oct. 20, 2009).

[132] YOMURI SHIMBUN, *supra* note 129.

[133] *Id.*

be a hard job tracking down each student's home on foot. So Google Maps is a convenient tool for finding houses and creating lists of locations just by inputting the relevant addresses."[134]

The teachers believed that the maps created for the home visits were only accessible by themselves but in fact, the maps, and the pupil's information, were accessible to the public.[135] The My Maps default setting is to make information available to the public unless the map creator says otherwise.[136] Once the teachers realized their mistake, they tried to delete the pupils' information but found that they were unable to do so.[137] The teachers' tried several times to delete the customized maps but to no avail.[138] Google stores My Maps information on two or more different servers and deletion problems occurred because a data record remained on one server even if a user has deleted it from another.[139] Companies and hospitals in Japan have also encountered similar issues using My Maps.[140] Sega, the Tokyo-based video game maker, discovered personal information from 115 job applications was accessible to the public and a Nagoya hospital revealed the names, and personal information of patients receiving artificial dialysis.[141]

C. Invasions of Privacy

The last example involves the more general notion of invasions of individual privacy, which is defined as "the wrongful intrusion by individuals . . . into private affairs with which the public has no concern."[142] Two examples below highlight general concerns of invasions of privacy.[143]

1. Celebrity Tracking

In 2006, the media gossip website, Gawker[144] launched a Google Maps based geo-mashup called Gawker Stalker.[145] Internet users pinpoint and record the location of celebrity sightings in either New York or Los Angeles.[146]

[134] *Id.*

[135] *Id.*

[136] *Id*. *See also* Google Code, Google Maps Data API: Developer Guide for Http Protocol, http://code.google.com/apis/maps/documentation/mapsdata/developers_guide_protocol.html (last visited Nov. 24, 2009) (describing how the Google maps data default settings make user inputted information available to the public).

[137] YOMURI SHIMBUN, *supra* note 129.

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id*.

[142] Wordnet, http://wordnetweb.princeton.edu/perl/webwn?s=invasion%20of%20privacy (last visited Nov. 24, 2009).

[143] The author acknowledges the voluminous case law and commentary relating to celebrities and invasions of privacy. However, these issues will not be addressed in this article.

[144] Gawker, http://gawker.com/ (last visited Nov. 24, 2009).

[145] Gawker, Gawker Stalker, http://gawker.com/stalker/ (last visited Nov. 24, 2009).

[146] Gawker, Introducing Gawker Stalker Maps, http://gawker.com/news/stalker/introducing-gawker-stalker-maps-160338.php (last visited Nov. 24, 2009) [hereinafter Gawker Maps].

Gawker aims to update a celebrity sighting within fifteen minutes of receiving it.[147] A person can text or email Gawker and provide them with details of the celebrity sighting, such as location, time, date and other information such as how the celebrity looked and who they were with at the time of the sighting.[148] The user provided information is then aggregated with Google Maps.[149] An Internet user can click on a hotspot listed on the Gawker geo-mashup to view the latest celebrity listings or click on a particular celebrity to view all of the sightings provided by Gawker contributors.[150]

Not surprisingly, Gawker Stalker has been subject to some criticism regarding the privacy and the safety of those celebrities sighted. Dominic Knight, a journalist of the Sydney Morning Herald, stated in his news blog

> In particular, it [Gawker Stalker] seems like a fantastic way to put mentally ill people in touch with the famous people they want to stab. One of the sightings on there at the moment is Christian Slater coming out of the Dakota – the same building John Lennon lived in when he was shot by a crazy fan.[151]

Jeff McIntyre a reporter for the Canadian Broadcasting Corporation also writes that "[t]he immediate media response has been loud and contagious, with publicists and celebrities expressing shock and disdain. Not only do the pinpointed map coordinates constitute a new invasion of privacy, they insist, but Gawker Stalker is potentially fomenting a DIY paparazzi movement."[152] As presaged in the McIntyre article, celebrities themselves have responded with some angst at the prospect of having their whereabouts tracked. Stan Rosenfield, who represents the interests of George Clooney, amongst others, has highlighted issues regarding the provision of information about individuals "it's [Gawker Stalker] conceptually bad because it provides information to people that they don't need to have," he says. "There's a reasonable expectation of privacy that anyone has—you, me or someone who makes $200

[147] Jonathan Zittrain, *Privacy 2.0*, U. CHI. LEGAL F. 65, 86 (2008) [hereinafter Zittrain, *Privacy 2.0*] ("Gawker strives to relay the sightings within fifteen minutes and place them upon a Google map, so that if Jack Nicholson is at Starbucks, one can arrive in time to stand awkwardly near him before he finishes his latte.").

[148] *See* Gawker Maps, *supra* note 146 (encouraging site goers to include details such as the time, location, and behaviour of the celebrities they spot).

[149] *Id*.

[150] *Id*.

[151] Dominic Knight, Google's Searching for Stalkers, http://blogs.smh.com.au/newsblog/archives/dom_knight/013909.html?page=2#comments (last visited May 19, 2009) ("As always, Google's got great technology, but serious privacy problems"). *I.d.* The criticism directed purely at Google is a little harsh given that the geo-mashup was actually created by Gawker but it does address an interesting issue, which is addressed below, namely how much responsibility should Google have as a technological facilitator of geo-mashups. *See* discussion *infra* Part V (suggesting that the problems the website causes are compounded by the fact that there is little or no redress or remedy available against the geo-mashup creators or the geo-mashup technological facilitators).

[152] Jeff McIntyre, *Stalk Market: Why Gawker.Com Is Putting the Fear in Celebrities*, CBA, Mar. 23, 2006, http://www.cbc.ca/arts/media/gawker.html. *See also* Igossip, GPS Images - Celebrity Tracking, http://igossip.com/gossip/GPS_Images_a_Celebrity_Tracking_Ali_Lohan/542043 (last visited May 19, 2009) (regarding an example of McIntyre's "DIY paparazzi movement").

billion. This is why people have unlisted phone numbers."[153]

The geo-mashup tracking phenomenon does not just involve high profile celebrities as it has also involved "urban eccentrics".[154] For example, FindHeMan[155] allows Internet users to tracks the whereabouts of a well-known Manhattan resident "who bears a distinct resemblance to the comic book hero [He-Man]."[156] Users are asked to email the Find He-Man website with updates of the latest sightings.[157] Once received, the geo-mashup aggregates the latest observation onto a Platial map showing the location sighting of "He-Man."[158] Spiegel also reports about a site called the Seattle Notables, which is similar to Find He-Man, allows users to track the whereabouts of readily identifiable, local individuals.[159]

In a slightly different vein to tracking the activities of celebrities or well-known local persons, the Celebrity Maps geo-mashup shows Internet users where well known celebrities reside.[160] The geo-mashup overlays residential address information on top of a Google Map to pinpoint the homes of celebrities.[161] Internet users enter a surname in the search field and the geo-mashup returns a list of celebrities with that surname.[162] A user then clicks on a particular celebrity and the geo-mashup aggregates the name of the celebrity, along with the celebrity's residential address, over the corresponding geographical point on Google Maps.[163]

D. Summary Analysis

Privacy concerns in privacy invasive geo-mashups involve the interlinking of personal information misuse and invasions of individual privacy. Regarding the latter, geo-mashups, such as Gawker Stalker, clearly raise privacy issues.[164] Putting aside the legal and policy sentiments regarding the privacy of celebrities, it does not take a major stretch of imagination to see how a similar tracking geo-mashup could be developed as a means to bully an

[153] Donna Freydkin & Olivia Barker, *At Gawker Stalker, a 'Big Whole To-Do' over the Mapping Feature*, USA TODAY, Mar. 28, 2006, http://www.usatoday.com/life/people/2006-03-28-gawker-sidebar_x.htm.

[154] Brendan Spiegel, *Websites Go Crazy Tracking Urban Eccentrics*, WIRED, April 30, 2008, http://www.wired.com/entertainment/theweb/news/2008/04/urban_eccentrics .

[155] Find He-Man, http://findheman.com (last visited May 19, 2009).

[156] Spiegel, *supra* note 154.

[157] Find He-Man, *supra* note 155.

[158] He-Man Sightings, http://platial.com/map/He-Man-sightings/42645 (last visited Feb. 19, 2010).

[159] Spiegel, *supra* note 154.

[160] Celebrity Maps Home Page, http://www.celebrity-maps.com/index.php (last visited Feb. 19, 2010) (search "celebrity names" for a specific celebrity and the geo-mash will bring up a Google Map image of the celebrity's address).

[161] Celebrity Maps About Us, http://www.celebrity-maps.com/about_us.php (last visited Feb. 19, 2010).

[162] Celebrity Maps Home Page, *supra* note 160.

[163] *Id.*

[164] *See* discussion *supra* Part III.C.1.

ordinary individual by constant tracking and surveillance[165] or to marginalize further, already marginalized communities.[166]

The issues involving personal information misuse are equally complex. The Japanese My Maps geo-mashup showed how easy it is to publish personal information inadvertently on geo-mashups.[167] Those problems were also borne out by the BNP geo-mashup.[168] Both examples demonstrate the complex issues involved in the removal of information after publication.[169] The common concern that all the geo-mashups share, albeit Gawker Stalker[170] to a lesser extent, is the aggregation of information, particularly personal information, with a residential address, that can lead to the identity of an individual, based on the information provided and the address location. Addresses are therefore an important aspect of the regulation of privacy in geo-mashups.

However, is an address itself personal information and therefore subject to privacy laws? The recent Australian Law Reform Commission ("ALRC") review of privacy[171] analyzed the complexities that emerge when trying to define an address as personal information

> 3.139 In the ALRC's view, information that simply allows an individual to be contacted—such as a phone number, a street address or an IP address—in isolation, would not fall within the proposed definition of 'personal information'. The *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. . . . Contact information may become 'personal information' in certain contexts, for example, once a mobile number is linked to a particular individual or the number can reasonably be linked to a particular individual. If an agency or organisation [sic] can reasonably ascertain the identities of direct mail recipients by linking data in the address database with particular names in the same or another database, that information is 'personal information' and should be treated as such.
>
> 3.140 As information accretes around a point of contact such as a

[165] Given the ubiquity of mobile/cell phones, the merger of mobile communications with social networking facilities and the easy transfer of data to geo-mashups, it seems to the author only a matter of time before geo-mashup bullies emerge. The ability to track bullied individuals and then provide location-tracking information with commentary, overlaid onto a geo-mashup for either for public or private use is now becoming a simple task. *See, e.g.* Jennifer Van Grove, *4 Teens Sued for Obscene Fake Facebook Profile,* MASHABLE BLOG, Sept. 25, 2009, http://mashable.com/2009/09/25/fake-facebook-profile (describing how four teenagers created a fake Facebook profile for another Illinois student, in order to harm his reputation).

[166] A website along the lines of TrackYourTramp.com is not a great a leap forward from the existing Seattle Notables geo-mashup. *See*, e.g., Adopt-a-Tramp, http://www.facebook.com/group.php?gid=8251968356 (last visited Oct. 20, 2009) (describing a Facebook business/public relations group).

[167] *See* discussion *supra* Part III.B.2.

[168] *See* discussion *supra* Part III.A.1.

[169] *See* discussion *supra* Part III.A.1.

[170] *See* Gawker, *supra* note 144.

[171] *See* AUSTRALIAN LAW REFORM COMMISSION, REP. NO. 108, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE (2008) [hereinafter AUSTRALIAN PRIVACY LAW AND PRACTICE] (regarding the final report); AUSTRALIAN LAW REFORM COMMISSION, DISCUSSION PAPER NO. 72, REVIEW OF AUSTRALIAN PRIVACY LAW (2007) [hereinafter ALRC DISCUSSION PAPER] (regarding the Commission's initial discussion paper).

> telephone number, an address, an email address or an IP address, it will become possible to link that information to a particular individual, to contact or affect that individual or to target the individual, for example, with advertising material. Once this occurs, that information becomes 'personal information' for the purposes of the *Privacy Act.*[172]

The ALRC states that where an individual's address presents with other information, which relates to that individual, then the likelihood increases that an individual's identity can be reasonably ascertained, especially if that individual can then be contacted.[173] Thus, the character of the information set as a whole tilts toward 'personal information.' From an information privacy perspective, addresses can act as an identifier to link different data sets together.[174] Because it helps 'accrete' data around pieces of information, linking datasets increases the likelihood that the identity of the subject is ascertainable from the set as a whole. The status of information as 'personal information' therefore has an important element of context, i.e., the context and inter-relationship of each of the available information components and the extent to which they collectively make identification possible.

Moreover, the use of geo-mashups exacerbates such issues because their use of information and their generation of visual content forces attention towards geography, particularly in the form of residential addresses. For example, the BNP membership list is a simple text file that merely provides a list of information that includes personal information.[175] It is of course possible to identify where a BNP member resides from the list but it is the generative exercise of enhancing and overlaying the raw text with an online map that re-emphasizes focus on cities, towns and individual residential addresses.[176] It is therefore not just the content of information that it is of concern but it is also the context of information use. Both of these situations arise in geo-mashups given the ease with which information can be aggregated onto maps that can have the effect of creating new information that is particularized around specific geographic points. It is this particularization that can give rise to enhanced privacy concerns regarding geo-mashups because, as highlighted by the ALRC above, access to addresses can enable identification.[177]

In terms of geo-mashups and identification, it is important to look beyond

[172] ALRC DISCUSSION PAPER, *supra* note 171, at 205.

[173] *See* AUSTRALIAN PRIVACY LAW AND PRACTICE *supra* note 171, at 299.

[174] *See* Roger Clarke, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, Roger Clarke's Web Site, http://www.rogerclarke.com/DV/Intro.html (defining information privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves").

[175] *See supra* note 30, and accompanying text.

[176] *See, e.g.*, TANASESCU, ET AL., *supra* note 36, at 247 ("The popularity of Web 2.0 maps and mash-up applications shows the interest and the appeal of the geographic environment for Web users; mash-ups are used for such a wide variety of goals that it seems that space, mediated through realistic Web maps, may provide the terrain for data integration rooted into human cognition that the more abstract textual Web has not yet succeeded to achieve.").

[177] *See* ALRC DISCUSSION PAPER, *supra* note 171, § 3.139-3.140.

the limited notion of identity as the ability to name, and thus identify an individual. Instead, geo-mashups underline the importance of a wider societal identity of a person as a constituent of the various wanted and unwanted meta-societies we live in, such as a member of the BNP, a reader of 'subversive' books or a rape victim.[178] Residential addresses provide access to ourselves by the ability to link the sensitive constituent meta-societies we reside in, to our identity, which can then be made available to a wider audience, outside the parameters of the meta-societies.[179] This brief discussion of the status of addresses highlights the limits of statutory privacy protection founded solely on the concept of information privacy and the overt focus on the collection and use of personal information. As highlighted in the next part, privacy invasive geo-mashups challenge the effectiveness of fair and lawful regulation of personal information exchange, based on the notion of fair information principles or practices. The next part of the article will draw on Zittrain's *Privacy 2.0* as a framework to highlight the difficulties that first generation privacy laws have regarding the regulation of privacy in Web 2.0 and with geo-mashups in particular.

IV. PRIVACY 2.0

In his 2008 article, *Privacy 2.0*, Zittrain contends that the unique issues raised by the generative web require new privacy solutions because first generation information privacy laws are fast becoming defunct against the issues arising from generativity.[180] Information privacy laws are concerned with regulating the relationship between individuals and powerful organizations about the provision and use of personal information. In new online structures, individuals, as well as organizations, collect and use personal information. Building on Zittrain's work, this part of the article will outline the foundations and legal principles of first generation information privacy laws before detailing Zittrain's criticism of them.

A. The Foundations & Legal Principles of First Generation Information Privacy Laws

Zittrain highlights the rise of privacy concerns in the 1970's generated by the advent of new computing technologies that enabled organizations to automate the collection of personal and non-personal information from

[178] *See* Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, 7 INFO. TECH. & PEOPLE 4, 6–37 (1994), *available at* http://www.rogerclarke.com/DV/HumanID.html#Bases (regarding the bases of human identification that recognize societal inputs above and beyond identification by name).

[179] *See* Gary T Marx, *What's in a Concept? Some Reflections on the Complications and Complexities of Personal Information and Anonymity*, 3 U. OTTAWA L. & TECH. J. 1 (2006) (regarding the value conflicts that can arise between the individual and the community regarding identity and anonymity).

[180] Zittrain, *The Generative Internet, supra* note 14, at 1980 (defining generativity as "a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences").

individuals.[181] Key reports and international instruments, from the early 1970's, through to the early 1980's, were instrumental in the development of first generation information privacy laws and thus addressed rising societal, governmental and institutional concern.[182]

In 1973, the US Department of Health, Education and Welfare produced a report entitled Records, Computers and the Rights of Citizens ("HEW Report").[183] The HEW Report's central apprehension was the relationship between individuals and recordkeeping organizations with regard to the "growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens."[184] The Report attempted to find a balance between the organizational benefits arising from the enhanced efficiencies of automated personal data processing and the potential infringement of personal liberties from impersonal data collection.[185] The balance was achievable through the concept of mutuality and by providing a degree of individual control over the collection of, access to, and disclosure of, an individual's personal information:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure[,] or use is specifically authorized by law.[186]

The Report concluded that existing laws provided inadequate protection of individual privacy against potential record-keeping abuses and recommended the establishment of a Federal "code of fair information

[181] Zittrain, *Privacy 2.0*, *supra* note 147, at 66–67.

[182] *See* Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99 (Philip E. Agre & Marc Rotenberg eds., MIT Press 1997) ("[S]trong pressures for 'policy convergence' had forced different states to legislate a broadly similar set of statutory principles to grant their citizens a greater control over personal information."); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L. J. 195, 200 (1992) ("[P]rivacy principles applicable to computer processing of personal information were widely recognized around the world as a necessity for an information-based economy.").

[183] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm [hereinafter HEW REPORT].

[184] *Id.*, at Preface.

[185] *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 195–96 (Philip E. Agre & Marc Rotenberg eds., 1997) ("[T]he executive and legislative branches looked at the increasing computerization of personal records and decided that new controls on technology were needed and that new protections for individuals were appropriate.").

[186] HEW REPORT, *supra* note 185, § III.

practice" for all automated data systems.[187] The HEW Report's recommendations led to the enactment of the Privacy Act of 1974 (US)[188] which established the recommended Code of Fair Information Practice for Federal Government agencies.[189] These five core principles of fair information practice are the:

1. *Notice/Awareness principle* requires organizations to give an individual clear notice about information practices before personal information is collected;[190]
2. *Choice/Consent principle* provides an individual the opportunity to consent to secondary uses of their information;[191]
3. *Access/Participation principle* ensures that an individual is able to access data about themselves to ensure that data is accurate and complete;[192]
4. *Integrity/Security principle* obliges an organization that collects personal data to take reasonable steps to ensure that the data is accurate[193] and is held in a secure environment;[194] and
5. *Enforcement/Redress principle* provides an individual with the means to enforce a breach of the principles.[195]

During the same period, the Committee of Ministers of the Council of Europe adopted two resolutions that concerned the protection of individual privacy arising from personal information held in private and public sector databases.[196] The resolutions were the instigator of "a more substantial legal instrument" to ensure adequate individual protections whilst enhancing the free trade of member countries.[197] In 1981, the Council of Europe formally adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* that extended the ambit of the previous Council Resolutions.[198] The Convention was intended as a catalyst to

[187] *Id.* § IX. *See* Gellman, *supra* note 185, at 195 ("A key objective of the Privacy Act was restricting the government's use of computer technology to invade privacy. This act was based on the 1973 recommendations of a federal advisory committee.").

[188] Privacy Act of 1974, 5 § U.S.C 552 (2006).

[189] *See* DANIEL J. SOLOVE, ET AL., INFORMATION PRIVACY LAW 578 (2006) (citing HEW REPORT, *supra* note 183 at 23–30, 41–42).

[190] 5 U.S.C. § 552(e)(3) (agency requirements).

[191] 5 U.S.C. § 552(b) (conditions of disclosure).

[192] 5 U.S.C. § 552(d) (access to records).

[193] 5 U.S.C. § 552(e)(6).

[194] 5 U.S.C. § 552(e)(9), (10).

[195] 5 U.S.C. 552(g) (civil penalties), (i) (criminal penalties),

[196] Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, Council of Europe Res. 73(22) (Sept. 18, 1973), *available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/internationallegalinstruments/1Resolution(73)22_EN.pdf; Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, Council of Europe Res. (74)29 (Sept. 16, 1974), *available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/internationallegalinstruments/1Resolution(74)29_EN.pdf.

[197] ROSEMARY JAY & ANGUS HAMILTON, DATA PROTECTION LAW AND PRACTICE 8 (3d ed. 2007).

[198] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. 108, available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

encourage and guide state legislative initiatives rather than to provide a readily implementable set of data protection rules and regulations,[199] as exemplified by the generality of the Convention's principles, namely, that personal information is to be:

1. Collected and processed in a fair and lawful manner;
2. Only stored for specified purposes;
3. Only used in ways that are compatible with those specified at the point of data collection;
4. Adequate, relevant and not excessive in relation to the purpose of data collection;
5. Accurate and where necessary kept up-to-date;
6. Preserved in identifiable form for no longer than is necessary;
7. Kept adequately secure; and
8. Accessible by individuals who have rights of rectification and erasure.[200]

Fourteen years later the European Community adopted the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[201] to create an EU wide regime that sets governance rules for member states to follow.[202]

The Organization for Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* crystallized transnational improvements in 1980.[203] The OECD recognized that the 1970s were an intensive period of legislative investigation and activity about the protection of privacy with respect to the collection and use of personal information.[204] Member countries of the OECD had a common interest in the protection of individual privacy and in the reconciliation of fundamental and competing values involved in automatic data processing and transborder flows of personal information.[205]

> For this reason, OECD Member countries considered it necessary to develop Guidelines, which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into

[199] LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 34 (2002).

[200] JAY & HAMILTON, *supra* note 197, at 8–9.

[201] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (EU).

[202] *See* BYGRAVE, *supra* note 164, at 58.

[203] ORG. FOR ECON. CO-OPERATION AND DEV. [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *available at* http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html [hereinafter OECD GUIDELINES].

[204] OECD GUIDELINES, *supra* note 203.

[205] Roger Clarke, *The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law*, http://www.anu.edu.au/people/Roger.Clarke/DV/PaperOECD.html (last visited Feb. 21, 2010).

> existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.[206]

As with the HEW Report and the Council of Europe Convention, the OECD Guidelines were concerned with the maintenance of balance.[207] On this occasion, the balance was between the harmonization of different legislation to protect privacy and to preserve the integrity of transborder flows of personal information.[208] The Guidelines were therefore an attempt to reduce the restrictions that inhibited the transfer of personal information and to strengthen the free information flow between member countries.[209] The OECD considered that this balance was achievable because

> [I]t is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. . . .
>
> Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.[210]

The Guidelines provided eight core principles of data collection, storage, and use for application by member countries, namely the:

> 1. *Collection limitation principle* which guarantees that the collection of personal data is within lawful and fair means, and where appropriate is conducted with the knowledge and consent of the individual;
> 2. *Data quality principle* which requires data collectors to collect personal data for relevant purposes only and to ensure that collected data is accurate, complete[,] and up to date;
> 3. *Purpose specification principle* which states that the purpose for which personal data is to be used must be stated at the time of collection and subsequent use must be limited to that purpose, unless individuals are notified of additional uses before that re-use takes place;
> 4. *Use limitation principle* which states that personal data should only be disclosed or used in accordance with the consent of the individual or by authority of law;
> 5. *Security safeguard principle* which requires that personal data must be kept in reasonably secure conditions;
> 6. *Openness principle* which states that organizations should implement a general policy of openness about data collection

[206] OECD GUIDELINES, *supra* note 203.

[207] *Id*.

[208] *Id*.

[209] *Id*.

[210] *Id*.

developments, practices and policies;

7. *Individual participation* principle which confirms that an individual should retain certain rights over the collection, storage and use of their information; and
8. *Accountability principle*, which confirms that a data collecting organization, should be accountable for complying with the above principles.[211]

The HEW Report, the Council of Europe Convention, and the OECD Guidelines have been at the forefront of the development of first generation information privacy laws. There are obvious similarities between the three documents that first generation information privacy laws reflect.[212] The HEW Report was directly responsible for the instigation of the Privacy Act of 1974, and the Convention eventually founded the European Union's Data Protection Directive. Furthermore, the OECD Guidelines have had a significant impact as a foundation for national legislation,[213] including Australia[214] and Canada.[215] All of these laws have organizational-oriented controls founded on the privacy principles or fair information practices developed in the previous decade.[216]

Bygrave[217] has adduced eight core legal principles that reflect the

[211] *Id.*

[212] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, STAN. TECH. L. REV 2 (2001)

> Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. . . . Commentators have also noted a remarkable convergence of privacy policies. Countries around the world, with very distinct cultural backgrounds and systems of governance, nonetheless have adopted roughly similar approaches to privacy protection. Perhaps this is not so surprising. The original OECD Guidelines were drafted by representatives from North America, Europe, and Asia. The OECD Guidelines reflect a broad consensus about how to safeguard the control and use of personal information in a world where data can flow freely across national borders.

Id.

[213] *See* BYGRAVE, *supra* note 199, at 32 (noting that the treaty has been ratified by twenty-seven member states).

[214] PRIVACY ACT 1988 (Austrl.). *See also* Greg Tucker, *Frontiers of Information Privacy in Australia*, 3 JLIS (1992) (regarding a brief history of the Act's development and the relationship with the OECD Guidelines).

[215] The PRIVACY ACT 1983 (Can.) was developed from the OECD Guidelines with reference to public sector privacy protection only. *See* Austin, *supra* note 77, at 123–4 (referring to the impact of the OECD Guidelines on the development of Canadian privacy law in general and the PIPED Act in particular).

[216] *See e.g.*, COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2d ed. 2006) (addressing policies of private protection of private information); Viktor Mayer-Schonberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 219, 221 (1997) (describing the European advances in data storage and protection).

[217] The author provides examples of Bygrave's principles with reference to four key first generation information privacy laws: the PRIVACY ACT 1974, the EU DATA PROTECTION DIRECTIVE, the PRIVACY ACT 1988 (Austrl.) and the PRIVACY ACT 1983 (Can.).

fundamental aims of first generation information privacy laws.[218] The primary principle is that personal information is to be "processed fairly and lawfully," and this concept manifests throughout the remaining principles.[219] The lawful element is apparent, that organizational personal information collection practices must be within existing law, but the fairness criterion is more abstract in nature, particularly because general agreement about what is fair will change over the course of time.[220] In general, the notion of fairness requires data collectors to take account of the interests and expectations of individuals who provide personal information to them.[221] Personal data collection organizations are therefore obliged not to pressure individuals when they provide their personal information and to ensure an individual consents to the provision.[222]

The minimality principle directs data collecting organizations to ensure that the collection of personal information is "limited to what is necessary to achieve the purpose(s) for which the data are gathered and further processed."[223] Under this principle, organizations are required to collect personal information only for a relevant purpose.[224] Linked to minimality, the purpose specification principle dictates that personal information is only collected for specified, lawful or legitimate purposes and can only be used within these bounds.[225] Bygrave states that the principle is essentially a cluster of three related sub-principles, namely that the data collection purpose is: (1) specified; (2) lawful and/or legitimate; and (3) that further personal data

[218] *See* Bygrave, *supra* note 199, at 57 (referring to data protection rather than information privacy laws); Simon Davies, Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in Technology and Privacy: The New Landscape 158 (1997) (regarding a critical distinction between the data protection and information privacy); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 Iowa L. R. 553, 560 (1995) (regarding a more positive view of data protection as the enhancement of participation in informational and political processes); Roger Clarke, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, http://www.rogerclarke.com/DV/Intro.html (last visited Feb. 23, 2010).

> Legislatures of countries on the Continent of Europe, and to some extent also in North America, passed laws addressing information privacy, primarily during the 1970s, though with some laggards deferring action until the 1980s or even 1990s. These laws mostly focus on 'data protection', i.e. they protect data about people, rather than people themselves. This is unfortunate because, although data protection is a more pragmatic concept than the abstract notion of privacy (and it's therefore easier to produce results), it's not what humans actually need.

Id. Clarke touches on the normative values of data protection laws as a protector of individual rights rather than the protection of personal data. In many ways, this type of protection is akin to that described by Zittrain in Privacy 2.0. Accordingly, for the purposes of this article, the author recognizes the distinctions that can arise from data protection and information privacy legal concepts but uses 'first generation information privacy laws' as a catch all for both types of law.

[219] Bygrave, *supra* note 199, at 58.

[220] *Id*.

[221] *Id*.

[222] *Id*. at 59. For example, 5 U.S.C. § 552(a)(b)(1)–(4); Council Directive 95/46, art. 6(1) & 7(1), 1995 O.J. (L 281) (EC); Privacy Act, R.S.C., ch. P–21, s. 7 (2009) (Can.); Privacy Act, 1988, s. 14 (Austrl.) Information Privacy Principles 1 & 9.

[223] Bygrave, *supra* note 199 at 59.

[224] *See, e.g.*, 5 U.S.C § 552(a)(b)(2) (2006); Council Directive 95/46, art. 6(1)(b)–(c), 1995 O.J. (L 281) (EC); Privacy Act, R.S.C., ch. P 21, § 5(1) (2009) (Can.); Privacy Act, 1988, s. 14 at 54 (Austrl.).

[225] Bygrave, *supra* note 199, at 61.

processing is compatible with the data collection purpose.[226]

The information quality principle ensures that personal information is accurate, both in terms of its content and context, and with regard to the purpose of information collection and processing.[227] The principle ensures that personal data is valid because it describes unambiguously what it pertains to and because it is relevant and complete with respect to the purposes of intended processing and use.[228] Information quality requires the participation of individuals to ensure that information held is up to date. Accordingly, the individual participation and control principle is pivotal because it ensures that persons have a measure of influence over the processing of their personal information by organizations and individuals.[229] However, most first generation information privacy laws do not refer to the principle directly.[230] Instead, legislation implicitly acknowledges the principle in legal rules that govern the collection, storage, and use of personal information in accordance with individual knowledge and consent.[231] Likewise, first generation laws rarely state the disclosure limitations principle directly but it implicitly requires data collecting organizations to restrict the disclosure of personal information within the confines of how data is collected, and within the consent provided by individuals or by the authority of a given law.[232] The two remaining principles, information security[233] and sensitivity[234] protect the integrity of personal information through the provision of adequate methods of security, particularly regarding sensitive information, which may require controls that are more stringent.

The historical development of first generation information privacy laws highlights that the collection, storage and use of personal information by data collecting organizations was the dominant concern of lawmakers and solutions to emergent problems lay in the construction of information privacy principles

[226] *Id*. *See, e.g.*, 5 U.S.C § 552(a)(b)(2); Council Directive 95/46, art. 6(1)(A), 1995 O.J. (L 281) (EC); Privacy Act R.S.C. ch. P-21, s. 4 (2009) (Can.); Privacy Act, 1988, s. 14 (Austl.) Information Privacy Principle 1.

[227] Privacy Act, 1988, s. 14 (Austl.).

[228] *See, e.g.*, 5 U.S.C. § 552(a)(e)(1),(5)-(6); Council Directive 95/46, art. 6(1)(d), 1995 O.J. (L 281/40) (EC); Privacy Act, R.S.Q., ch. P 21, s. 4-5 (2009) (Can.); Privacy Act, 1988, s. 14 (Austl.), Information Privacy Principle 3.

[229] *See* BYGRAVE, *supra* note 199 at 63.

[230] *Id. See, e.g.*, 5 U.S.C. § 552(a)(c)(1)-(4); Council Directive 95/46, art. 10, 12, 1995 O.J. (L 281/41-42) (EC); Privacy Act, R.S.Q., ch. P 21, s. 12(1)(A)-(B) (2009) (Can.); Privacy Act, 1988, s. 14 (Austl.), Information Privacy Principles 5–7.

[231] *See* BYGRAVE, *supra* note 199 at 63. *See, e.g.*, 5 U.S.C. § 552(a)(c)(1)-(4); Council Directive 95/46, art. 10, 12, 1995 O.J. (L 281/41-42) (EC); Privacy Act, R.S.Q., ch. P 21, s. 12(1)(A)&(B) (2009) (Can.); Privacy Act, 1988, s. 14 (Austl.), Information Privacy Principles 5–7.

[232] *See* BYGRAVE, *supra* note 199 at 67. *See, e.g.*, 5 U.S.C. § 552(a)(e)(9)-(10); Council Directive 95/46, art. 17, 1995 O.J. (L 281/43) (EC); Privacy Act, R.S.Q., ch. P 21, s. 6(3) (1985) (Can.); Privacy Act, 1988, s. 8(1)-(2) (Austl.), Information Privacy Principle 4.

[233] *See* BYGRAVE, *supra* note 199 at 67. For example, the information security principle is not recognised as fully as the other principles.

[234] *See* BYGRAVE, *supra* note 199 at 68; Marx, supra note 175, at 13 (demonstrating the rationale for greater control over personally sensitive information); Council Directive 95/46, art. 8(1), 1995 O.J. (L 281/40) (EC).

or fair information practices.[235] Such regulation was possible because the social modes of personal information provision, process and use were predictable, stable, and relatively static.[236] Public and private sector organizations were the main collectors of personal information for clearly defined purposes.[237] As such, the imposition of fairness upon the procedures of personal information collection and use was possible because those procedures were identifiable and therefore manageable. Information privacy regulation was able to find a balance, or a compromise, between the societal concerns of individuals that provided their personal information and the organizations that required personal information to fulfill their business or statutory purpose. However, Web 2.0 has distorted the balance because new information relationships require new forms of privacy regulation as outlined in Zittrain's *Privacy 2.0*.[238]

B. Zittrain's Criticism of First Generation Laws

Zittrain has two principal criticisms about the ineffectiveness of first generation information privacy laws in newly, evolving Internet structures.[239] The first regards the new information exchange relationships that emerge from Web 2.0 which are more complex than the traditional personal data collection pathways of the previous decades.[240] The second contends that individual, as well as organizational actions, can now give rise to an equal number of privacy concerns.[241] New technological developments and social structures mean that individuals now have the same capacity to infringe the privacy of individuals as organizations once did.[242]

Zittrain argues the privacy problems that arise from Web 2.0 related technologies and cultures require new solutions because existing laws only provide remedies for older ideas of privacy predicated on the concept of information privacy. Such laws safeguard an individual's privacy by providing

[235] DANIEL J. SOLOVE ET AL., *supra* note 185, at 578–79.

> Fair Information Practices can be understood most simply as the rights and responsibilities that are associated with the transfer and use of personal information. Since the intent is to correct information asymmetries that result from the transfer of personal data from an individual to an organization, Fair Information Practices typically assign rights to individuals and responsibilities to organizations.

Id.

[236] *See, e.g.,* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* 53 STAN. L. REV. 1393, 1400–413 (2001) (providing a historical overview of governmental and private sector personal information collection and legal impacts through notions of Big and Little Brother focused regulation).

[237] *See* ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY 66–75 (1972) (regarding disclosures of personal information that may have been flexible but the pathways of personal information provision which were relatively static, as in the New York State Department of Motor Vehicles (DMV) case study).

[238] Zittrain, *Privacy* 2.0, *supra* note 147, at 65.

[239] *Id*.

[240] *Id.* at 74.

[241] *Id.* at 65.

[242] *See, e.g.,* Owad, *supra* note 101 (regarding the use of home computer equipment for relatively complex data mining purposes).

protections relating to the collection, storage and use of personal information along well-established data provision pathways. These laws thus recognize that there is a degree of social sensitivity attached to the production of personal information and that organizational activities relating to personal information should be restricted to legally mandated, legitimate means.[243]

Legal remedies designed in the 1970's and 1980's, may therefore provide ineffective and rigid solutions to personal information exchange problems in Web 2.0. The first generation of information privacy laws focused on the regulation of three stakeholder groups involved in personal information provision. The three groups in question are of course, those individuals[244] who provide personal information,[245] personal data collecting organizations[246] and finally, a further set of organizations that use personal information previously collected, by their own or by different organizations, that has been disclosed to them.[247] Legal controls attempt to regulate the activities between individuals and organizations within two binary relationships: the first between the data provider and the data collector and the second between the data collection organization and the data re-user organizations. A chain of accountability links all three groups to ensure that personal information provided by individuals is collected and stored within certain legal boundaries.[248] Moreover, personal information provided by individuals is stored with legally requisite standards to ensure the accuracy and the security of the information.[249] Finally, future re-uses of provided personal information are circumscribed within specific confines, to ensure that the information collected can only be used for the purpose for which it was originally collected[250] or under a specified exemption to that purpose.[251]

However, first generation legal controls may now be ineffective because

[243] *See* Zittrain, *Privacy 2.0, supra* note 147, at 69 (discussing the tension between the utility of electronic consumer data gathering and privacy concerns).

[244] For example, using the four laws highlighted above, in 5 U.S.C § 552(a)(2) "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence; in Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) (EC) "data subject" means an identified or identifiable natural person; in Privacy Act, R.S.C., ch. P-21 (2009) (Can.) "individual" is undefined; and in Privacy Act, 1988, s. 6 (Austl.) "individual" means a natural person.

[245] The type of information or data covered by first generation laws varies. *Compare, e.g.*, Privacy Act, 1988, s. 6(1) (Austl.) (referring to "personal information") *with* Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) (EC) (referring to "personal data").

[246] The definition of the organization can vary by country. *See* 5 U.S.C § 552a(a)(9), (11) (referring to "source" and "recipient agency"); Council Directive 95/46, art. 2(e)-(g), 1995 O.J. (L 281) (EC) (referring to "processor", "third party" and "recipient"); Privacy Act, R.S.C., ch. P-21, s. 2 (2009) (Can.) (referring to "government institution"); Privacy Act, 1988, s. 3(a) (Austl.) (referring to "agency" or "organisation").

[247] This class of organization can vary by country. *See* 5 U.S.C § 552a(a)(e)(9)-(10) (referring to "recipient agency," and "non-federal agency"); Council Directive 95/46, art. 17, 1995 O.J. (L 281) (EC) (referring to "member states," "controller[s]" and "processor[s]"); Privacy Act, R.S.C., ch. P-21, s. 3 (2009) (Can.) (referring to "government institution"); Privacy Act, 1988, s. 6 , s. 3(a) (Austl.) (referring to "agency" or "organisation").

[248] *See, e.g.* BYGRAVE, *supra* note 199 (regarding the minimality and purpose specification principles).

[249] *See Id*. (regarding the information quality, individual control and participation, information security and sensitivity principles).

[250] *See Id*. (regarding the individual control and participation principles).

[251] *See Id*. (regarding the disclosure limitation principles).

Web 2.0 enables multiple information contributions from a range of different and unconnected sources. As Zittrain states, "[t]he heart of the next generation privacy problem arises from the similar but uncoordinated actions of individuals that can be combined in new ways thanks to the generative Net."[252] First generation laws envisage selected pathways of personal information provision and distribution. The move from binary to multiple pathways of personal information provision and use has been brought about and created a situation in which "the Net puts private individuals in a position to do more to compromise privacy than the government and commercial institutions traditionally targeted for scrutiny and regulation."[253] As such, Web 2.0 now delivers many different pathways because individual Internet users are now the collectors, disseminators, and re-users of personal information.

One of the key points of concern arising from Zittrain's Privacy 2.0 therefore involves the governance of ever developing information pathways that enable the collection, storage, and use of personal information from individuals, by other individuals.[254] The once clear cut boundaries have been blurred to the extent that Internet personal information users are no longer just organizations but are now inchoate collections of far flung individuals, who coalesce in different groups to use and share their own and other individual's personal information.[255] These collectives are themselves "databases [that] are becoming as powerful as the ones large institutions populate and centrally define".[256] Except the power to infringe personal privacy within these new data collectives is different from the fears of the 1970's and 1980's. The flows of personal information into and out of these collectives are multiple, diffuse, erratic and serve many different purposes of collection and subsequent re-use. Contrast that to the concerns of first generation laws in which monolithic organizations collected personal information for specific purposes, largely direct from the individuals themselves and whose subsequent re-use of personal information was mostly predictable.[257]

[252] Zittrain, *Privacy 2.0*, supra note 147, at 65.

[253] *Id.*

[254] *See Id.* at 81 (stating "[w]ith cheap sensors, processors, and networks, citizens can quickly distribute to anywhere in the world what they capture in their backyard. Therefore, any activity is subject to recording and broadcast".

[255] *See Id.* at 100 (discussing the personal information on databases that are produced and continually changing on peer-produced social groups such as Facebook and MySpace).

[256] *Id*. at 99.

[257] Personal information disclosure has historically been more difficult to approximate than personal information collection because of the different uses that personal information can be put to. However, privacy concerns regarding the disclosure and the re-use of personal information can still fall into a relatively small number of categories, particularly surveillance, data matching and commercial purposes. *See e.g.* Austin, *supra* note 77, at 143 (regarding the major concerns arising from public and private sector personal data collection); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement* 29 N.C.J. INT'L L. & COM. REG. 595, 595–96 (2004) (showing how Choicepoint, a commercial database, makes available a wide array of information); Gary T. Marx, *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, 59 J. SOC. ISSUES., 370 (2003) (regarding general surveillance concerns); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J., 1321, 1329–34 (1992)

Accordingly, the fundamental analytical template of first generation information privacy laws regarded the fact that "both the analysis and suggested solutions speak in terms of institutions gathering data, and of developing ways to pressure institutions to better respect their customers' and clients' privacy".[258] This basic template has shaped the development of privacy legislation during the last three decades but has not effectively made the transition from "a functional theory to a successful regulatory practice".[259] In fact, some commentators argue that business interests have skewed the balance sought from first generation laws.[260] However, the very notion of what a business organization is has itself changed, and continues to change, in new online structures. With that comes changes in business technologies and techniques, as can be seen with the very foundation of first generation concerns, the database, which is now almost in "constant beta" to the extent that "how a database is defined, changes from one moment to the next, both in terms of content, structure and scope."[261]

First generation fears focused on powers arising from the centralization of personal information and nefarious uses by powerful organizations without the knowledge, input or consent of individuals. The first generation information privacy laws were an attempt to manage disputes arising between individuals and organizations about a contested social asset, an individual's perceived right of control over their personal information against an organization's economic need to use that information. Contested issues were disputed within a scenario of clearly identifiable actors, accepted definitions of personal information and evident, yet limited legal rights and obligations. Privacy 2.0 concerns, on the other hand, manifest through peer-to-peer technologies that eliminate points of control regarding the transfer of personal information.[262] Whilst the contested social asset is still personal information, the contests that are now developing in Web 2.0 are not about the fair or unfair processes of organizational personal information collection, but rather, they are about the socially acceptable re-uses of personal information by individuals in multiple, generative guises. Therefore, unlike their predecessors, Privacy 2.0 contested issues do not involve disputes between individuals and organizations in clear-cut, readily

(regarding the reasons for public sector personal information collection); Solove, *supra* note 236, at 1395 (regarding the scale of commercial re-use of personal information that causes current privacy problems and not just the commercial activity itself); Derek J Somogy, *Information Brokers and Privacy*, 1 I/S: J. L.& POL'Y FOR INFO. SOC'Y 901, 904–06 (2006) (regarding the rise of data brokers whose scale of development may not have been fully appreciated in the 1970's).

[258] Zittrain, *Privacy 2.0 supra* note 147, at 69.

[259] *See id*. at 68 (citing pressures arising from law enforcement and commerce as significant reasons for these failures).

[260] *See, e.g.*, DAVIES *supra* note 218; Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127 (2006); Solove, *supra* note 196; Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 379 (Jane K. Winn ed., 2006) [hereinafter Hoofnagle, *Privacy Self-Regulation*]. *available at* http://epic.org/reports/decadedisappoint.pdf.

[261] *See* Zittrain, *Privacy 2.0*, *supra* note 147, at 100 (discussing the dynamic nature of databases today and the unknown or secret depository of information users have on one another).

[262] *Id.* at 81.

identifiable scenarios founded on stable and largely one dimensional information pathways. Instead, disputes arise within webs of diverse individual Internet users within which numerous problems arise in unimagined scenarios. The next part of the article examines the BNP geo-mashup situation to show the change from binary to multiple information relationships and the increasing involvement of individuals as potential infringers of individual privacy.

V. THE BNP GEO-MASHUP: FROM BINARY TO MULTIPLE PERSONAL INFORMATION RELATIONSHIPS

In the BNP geo-mashup, we see a situation that highlights the limits of first generation information privacy laws when faced with a privacy invasive geo-mashup. As suggested by Zittrain, the key reason is the informal personal information dissemination pathways that were developed post publication of the membership list which effectively eliminated any vestige of control that BNP members may have thought they had over their personal information. While some forms of first generation legal redress are still available to individual BNP members, via obligations imposed on the BNP as a data collector, there is little or no redress or remedy available against the geo-mashup creators or the geo-mashup technological facilitators, Wikileaks and Google Maps.

The original act of personal information provision took place when an individual joined the BNP. In doing so, he or she provided the party with their personal information and that provision and collection of personal information was covered by the relevant privacy legislation, in this case the Data Protection Act of 1998.[263] The minimality and purpose specification principles' govern the act of personal information provision between the individual and the collecting organizations, which thus creates an information exchange relationship between them. These principles ensure that the BNP collects and processes personal information in a fair and reasonable manner. Furthermore, the information quality, individual control, and participation principles oblige the BNP to ensure that any collected personal membership information is kept accurate by reference to the individual who has provided that information. In so doing, an individual BNP member is able to ascertain from the BNP what personal information the BNP holds so that he or she can check the accuracy of that information, at any given time. Moreover, the information security and sensitivity principles mandate the BNP to keep personal information supplied by its members in a secure environment.

In the BNP example, the BNP conclusively failed to secure the personal information of its members because a disgruntled employee was able to gain unauthorized access to the BNP membership list. Furthermore, once the disgruntled employee gained access to the list, he or she was then able to copy

[263] Data Protection Act, 1998, c. 29, (U.K.) *available at* http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

it and to take it outside of the control of the BNP. At this point, first generation information privacy laws, founded on the core principles highlighted above, would continue to operate relatively effectively. The principles, and their concomitant laws, could not have stopped the willful unauthorized access by the disgruntled employee but the laws would provide some sort of recourse for those individuals who provided information to the BNP under a breach of the information security principle.[264] The primary reason for the effectiveness of the laws is a clear and unambiguous binary relationship between the individual BNP member and the BNP, as a data collector.

However, the binary relationship between the data collector and the data re-user fails to manifest under first generation laws because of the unauthorized breach by the disgruntled employee. The disclosure limitation principle that is central to the relationship between the BNP and subsequent information re-users fails to materialize in the absence of a binary relationship. BNP members therefore have little or no recourse against the BNP or subsequent information re-users under first generation laws. Nevertheless, there were a number of information re-users in the BNP example because Wikileaks, various geo-mashup creators, and Bit Torrent websites re-used the personal information of BNP members in a number of different ways.

Accordingly, there is an absence of one of the key links in the chain of accountability. The information re-users have no link with the data collection organization, the BNP, but more importantly, they have no link with the data provider, individual BNP members. Putting aside the misuse of personal information by the disgruntled BNP employee,[265] the first re-use took place when Wikileaks published the BNP membership list on their website. The second re-use then saw various individuals copying the membership list and placing it on BitTorrent websites for the purpose of wider distribution. News of the story then broke on various blogs. The third reuse of the BNP membership list arose when media outlets and individuals aggregated the BNP

[264] In fact, in some ways it could be argued that the Data Protection Act provided strong privacy protections given the arrest of the two individuals who were alleged to have been responsible for the unauthorized leak of the membership list. The arrests were presumably under offenses related to section 55(1) and (3) of the Act, "A person must not knowingly or recklessly, without the consent of the data controller—(a) obtain or disclose personal data or the information contained in personal data, or procure the disclosure to another person of the information contained in personal data." Section 55(3) states "A person who contravenes subsection (1) is guilty of an offence." *Id.* § 55(1), (3).

[265] It should be noted that the lack of a data breach notification law in the U.K. might also have exacerbated the problem particularly in light of the reporting to law enforcement agencies suggested. *See, e.g.*, Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L.R. 913 *passim* (2007) (discussing current state and federal data breach notification laws). If law enforcement agencies had been notified at the onset of the problem then perhaps action could have been taken to restrict the use of names and addresses. This is a debatable point given the fact that the effectiveness of data breach legislation remains in question. *See, e.g.* Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 726 (2007) (suggesting that it would be premature to judge the effectiveness of data breach legislation at this time); Kathryn E Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM. L. REV. 355, 390 (2006) (recommending that federal data notification breach legislation be supplemented with common law remedies to provide the most effective consumer protection).

membership list with Google Maps to create the geo-mashups highlighted above.

The original misuse of personal information by the disgruntled BNP employee infringed the privacy of BNP members through unauthorized access to their information and subsequent disclosure. However, it is the use of the BNP membership list, as a foundation stone for geo-mashups, which brings the situation to the fore and exacerbates the privacy infringements of BNP members, particularly in the case of the BNP Proximity Search geo-mashup.[266] Yet there is little or no recourse against Wikileaks, the creator of the geo-mashup or the facilitator of the geo-mashup, Google, under first generation information privacy laws because of the absence of a binary relationship between the information collector and the information re-user, even though issues arise under the information quality principle. For example, it is unclear whether the BNP Proximity Search geo-mashup aggregated the BNP list by postcode or by house number and street address. The residential properties pinpointed on Google Maps could either be (a) the address of a BNP member or (b) an out of date address for a BNP member or (c) the address of an individual who has nothing to do with the BNP but has the misfortune of having his/her house automatically tagged with a certain postcode by Google Maps.[267] All scenarios are feasible given the problems that arose from the BNP "Near Me" geo-mashup and the fact that the BNP admitted that the membership list was out of date.

The BNP Proximity Search raises specific privacy concerns regarding the use of sensitive and personal information, in the form of political party membership, names and addresses. The geo-mashup identifies members of the BNP by name and address. However, it is the aggregation and overlay on to Google Maps that causes greater concerns, particularly in combination with Google Street View, because the geo-mashup enables any person to identify the location of a BNP member at a particular house.[268] Furthermore, specific issues relating to the use and development of geo-mashups arise because the generative re-publication of information itself can give rise to inaccuracies.

[266] *See* TANASESCU, ET AL, *supra* note 36, at 247 (regarding reasons for the popularity of geo-mashups that add another, easier to understand dimension to the written words of the Internet).

[267] A car bombing attack provides a graphic example of the dangers arising from the provision of inaccurate information. The car attacked was owned by a neighbor of a BNP member and he had parked his car outside of his neighbor's house. According to the BBC, the BNP reported that none of its members lived on the street where the attack took place even though one of the houses in the street was on the BNP membership list. BBC NEWS, *supra* note 96. *See also* Paul Sims, *Police Probe 'Vigilante Firebomb' Attack on Home of Man Named on BNP List*, DAILY MAIL, Nov. 22, 2008, http://www.dailymail.co.uk/ news/article-1088167/Police-probe-vigilante-firebomb-attack-home-man-named-BNP-list.html (reporting the person who was named on the BNP list and his confirmation that he left the Party the previous year).

[268] Google Street View itself has been subject to some criticism. S*ee Greece Puts Brakes on Street View*, BBC NEWS, May 12, 2009, http://news.bbc.co.uk/2/hi/technology/8045517.stm (regarding the banning of Street View in Greece); Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet,* 49 SANTA CLARA L. REV. 313, 354–91 (2009) (regarding the development of a privacy related tort, "the right to your digital identity," in public places to counteract problems emerging from Google Street View). *But cf. All Clear for Google Street View,* BBC NEWS, April 23, 2009, http://news.bbc.co.uk/2/hi/technology/8014178.stm (regarding a decision by the U.K. Information Commissioner to pass its use in the U.K.).

For example, as highlighted by the BNP "Near Me" geo-mashup, the simple use or misuse of a specific type of marker, such as a pointer or a hot spot, can give an inaccurate representation of an otherwise accurate piece of information. Additionally, any inaccuracies in the BNP membership list will automatically be replicated in any subsequent geo-mashup. As such, it is astonishing to think that, at the time of writing, the BNP Proximity Search is still online and is still identifiable through Internet search engines.[269]

Referring back to Zittrain's work, the BNP example shows the limits of information privacy laws based on first generation principles because of the difficulties faced in applying founding maxims to generative systems of distributed personal information.[270] The definitional founding blocks of first generation regulation—personal information, records, databases, data subjects, collectors, and users—are becoming so diffuse that the core concepts of first generation laws are themselves changing from one moment to the next. To the extent that the concept of privacy regulation, like Web 2.0 technologies and structures, is now entering a period of constant beta, the developments of the online world are far outpacing the decades old laws that are currently being used to regulate it.[271] This raises serious questions about the ability of privacy laws predicated on the concept of technological neutrality[272] and their ability to keep pace with developments in Web 2.0, 3.0 and beyond.

VI. PRIVACY 2.0 SOLUTIONS FOR PRIVACY INVASIVE GEO-MASHUPS: EMBEDDED TECHNICAL & SOCIAL STANDARDS

If the intention of first generation laws is to regulate the relationship between individuals and powerful, monolithic organizations, how then should Privacy 2.0 attempt to govern disparate collectives of information collecting individuals and individuals themselves? Zittrain contends that the levels of privacy responsive regulation has to be lower for individuals than for organizations, otherwise the burden of compliance becomes so great that it

[269] The author has not included details of websites where the membership list is still available for obvious reasons but these sites are accessible via Internet search engines.

[270] *See* Zittrain, *Privacy 2.0*, *supra* note 147, at 100 (stating that generative systems of personal information distribution generate an ever-changing "database").

[271] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003) (referring generally of the societal issues involved with privacy regulation that require flexible and new approaches).

> If we look at the way in which information is collected and used in today's society, we see that the problems presented are not typical consumer issues that we can expect individuals to police for themselves with the aid of prohibitory laws. The policy issues have much more in common with societal problems that we have historically regulated in a fundamentally different way. Policy makers should recognize this relationship in the formulation of privacy legislation and create a regulatory environment that provides meaningful protection of our collective privacy interests.

Id.

[272] *See, e.g.*, AUSTRALIAN PRIVACY LAW AND PRACTICE, *supra* note 171, at 422 (enshrining the idea of technological neutrality in Australian privacy law) ("In the ALRC's view, technology-neutral privacy principles provide the most effective way to ensure individual privacy protection in light of developing technology.").

effectively restricts taken-for-granted Internet activities.[273] Abundant over regulation of individuals from an overtly complex privacy regime is dangerous because it has the capacity to frustrate the "generative developments" of individual users.[274] This part explores this idea in further depth to suggest embedded technical and social standards as potential solutions to mitigate the negative consequences of privacy invasive geo-mashups. However, in concluding this part, the author suggests that while embedded solutions, developed through discourse and interaction, would go some measure toward alleviating concerns, such standards must still be enmeshed in a legal framework to ensure effective protections and remedies.

A. Technical Solutions

Zittrain uses Creative Commons licenses as a potential template for privacy-related code-backed norms.[275] He argues that Creative Commons licensing has become popular on the Internet because they provide a collective signal to share information within agreed social boundaries.[276] Creative Commons[277] is a worldwide social project, embodied as non-profit organizations in different countries,[278] that operates to enhance the widespread use of creative output into "the commons – the body of work that is available to the public for free."[279] One of the key aims of the Creative Commons project is "to make copyright material more accessible and negotiable in the digital environment."[280] Creative Commons attempts to achieve this aim by making available to the public a license from which content users can attribute certain terms regarding the re-use of their material or information. For example, if a user's content is re-used by a third party then the third party may be required to attribute the original content creator, or a user can ensure that their content is not used for commercial purposes. As such, "the content owner reserves some rights of control but eschews the common commercial approach of all rights reserved."[281] Building on this approach, Zittrain contends that it is not the threat of legal sanctions that gives Creative Commons licenses weight, but rather, it is the capacity to touch into a "cultural mindshare" of web users.[282]

[273] *See* Zittrain, *Privacy 2.0*, supra note 147, at 99 (discussing how such regulation would effectively amount to a ban on information collection by non-institutional collectives of individuals).

[274] *Id.*

[275] *Id*. at 109.

[276] *Id*.

[277] Creative Commons, http://creativecommons.org (last visited Sept. 30, 2009).

[278] *See* Creative Commons, International, http://creativecommons.org/international (last visited Sept. 30, 2009) (displaying the mission of the organization and tools available for download); Creative Commons Australia, http://www.creativecommons.org.au (last visited Sept. 30, 2009).

[279] Creative Commons, What is CC?, http://creativecommons.org/about/what-is-cc (last visited Sept. 30, 2009).

[280] BRIAN FITZGERALD, OPEN CONTENT LICENSING: CULTIVATING THE CREATIVE COMMONS 3 (Sydney Univ. Press 2007).

[281] *Id.*

[282] Zittrain, *Privacy 2.0, supra* note 147, at 104─105.

Creative Commons licenses reside in the realm of intellectual property and a number of journal articles have already examined the copyright issues that arise from mashups and Web 2.0.[283] Whilst many of the same issues of information usage appear to be similar, the purpose and use of intellectual property and privacy regulation are so different that they do not offer grounds for clinical comparison.[284] However, Zittrain considers the use of Creative Commons licenses in a broad sense, not as a way to enforce rights over the protection of personal information *per se*, but as a potential template that would enable individuals to express preferences about how search engines should use and index their personal information.[285] Accordingly, in this context, Zittrain suggests the use of Creative Commons licenses as a readily available and popular template as a potential medium for individuals to specify their privacy preferences rather than an intellectual property based legal solution to enhance Privacy 2.0 solutions.[286] The lack of a privacy preference tool for Internet users inhibits meta-data transfer that could enable a two way passing of information about the agreed uses of personal information.[287] Zittrain argues that tagged meta-data would provide a way for individuals to signal whether they would like to remain associated with information they place on the web and to be consulted about any unusual future uses.[288] Privacy tags would promote respect regarding the uses of personal information on the Internet by creating a means "that connects and sets informal standards for distant and disparate individuals about the use and re-use of personal information".[289] Such tags would generate "privacy spaces" and would thus become the touchstone privacy tool of Web 2.0 by creating points of connection and accountability for Internet users who produce, transform and consume personal information.[290]

Warner and Chun have also developed the notion of privacy spaces in

[283] *See, e.g.,* Veasman, *supra* note 20; Lee, *supra* note 21; Branwen Buckley, *Suetube: Web 2.0 and Copyright Infringement*, 31 CVLAJLA 235 (2008); Greg Lastowka, *User-Generated Content and Virtual Worlds*, 10 VAND. J. ENT. & TECH. L. 893 (2007); Steven Hetcher, *User-Generated Content and the Future of Copyright: Part One - Investiture of Ownership*, 10 VAND. J. ENT. & TECH. L. 863 (2007); Steven Hetcher, *User-Generated Content and the Future of Copyright: Part Two - Agreements Between Users and Mega-Sites Symposium Review*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 829 (2007); Casey Fiesler, *Everything I Need to Know I Learned from Fandom: How Existing Social Norms Can Help Shape the Next Generation of User-Generated Content Note*, 10 VAND. J. ENT. & TECH. L. 729 (2007).

[284] *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1297 (2000) (highlighting deficiencies in the inter-changeability of copyright and information privacy concepts); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1147 (2000) (rejecting the concept of propertizing personal information); Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 USFLR 634 (2000) (contending the opposite view).

[285] *See* Zittrain, *Privacy 2.0, supra* note 147, at 106.

[286] *Id.* at 104–105.

[287] *Id.* at 106.

[288] *Id.* at 107.

[289] *Id.* at 109.

[290] *Id.* at 118.

mashups founded on government provided information.[291] Their concept aims to ensure privacy protection through the interaction of different privacy policies that represent the interests of different parties involved in a mashup process.[292] This combination of different privacy policies:

> [A]llows a user, as a data owner, to describe their privacy preferences as Personal Privacy Policies (PPP), government agencies, as data providers, to specify Regulatory Privacy Policy (RPP), and mashup service provider to specify their privacy policy (MPP). . . .
>
> The proposed technology solution includes a PPP network where citizens can register their personal privacy preferences, and a Privacy Enforcement engine that interprets PPP, RPP and MPP before releasing individual's data requested by third party applications such as mashups.[293]

The real time interaction of interrelated privacy policies builds boundaries between what individuals want to be kept private and information that can legitimately be used for public purposes. Warner and Chun recognize the privacy problems arising from mashups by the fact that individuals who provide personal information have virtually no control over who will be able to access their information once it is aggregated in a mashup.[294] Their remedy to this problem is to place limits on the use of personally identifiable information in mashups by the extensive use of a range of privacy policies "that enforce a situation in which an individual has the right to control information about them".[295] As such, internal data flows that found geo-mashups should be controlled, to adhere to the privacy requirements expressed by individuals and government agencies.[296]

The notions of individual control over information and the use of privacy policies are hallmarks of first generation laws, and Warner and Chun's work develop first generation concepts in interesting and novel ways. However, when faced with privacy invasive geo-mashups, such as the BNP geo-mashup, the bounds of protection are limited because their work focuses on personal information provided to and supplied by government organizations. A network of privacy preferences and policies may provide "multiple protection spaces [that allow] private data to be shared under certain protection spaces and not in others,"[297] but information sharing is based on the idea of a limited number of stable and identifiable information pathways. For instance, the authors state that:

[291] Janice Warner & Soon Ae Chun, A Citizen Privacy Protection Model for E-Government Mashup Services (2008), *available at* http://delivery.acm.org/10.1145/1370000/1367866/p188-warner.pdf?key1=1367866&key2=0455350721&coll=GUIDE&dl=GUIDE&CFID=83050524&CFTOKEN=90806981; Janice Warner & Soon Ae Chun, *Privacy Protection in Government Mashups*, 14 INFORMATION POLITY (2009) [hereinafter Warner & Chun, *Government Mashups*].

[292] Warner & Chun, *Government Mashups*, *supra* note 245, at 88.

[293] *Id.*

[294] *Id*. at 76.

[295] *Id*. at 79.

[296] *Id*. at 80.

[297] *Id*. at 82.

> The [Personal Privacy Policies] network will allow citizens to have more control over their own private data, through direct participation in protecting the private data. This participatory privacy protection also accommodates a high degree of individual differences in privacy, and may foster the level of trust in government agencies. It also simplifies the requirements on individuals. They can specify their preferences once for all known as well as unknown potential uses of their data.[298]

It may be possible for an individual to specify their preference for known uses of their personal information but how is an individual expected to specify their preference for an unknown use of their personal information? Take, for example, the BNP geo-mashup scenario. An individual BNP member may have been able to stress the limits on the use of their personal information by the BNP. They could state in their personal privacy policy that they do not want their information used in any subsequent geo-mashup created or authorized by the BNP. However, in this situation, personal privacy preferences would have become defunct once the disgruntled BNP employee accessed and used the membership list without authorization. A personal privacy policy could envisage a future use by the BNP within its own organizational standards, membership expectations, and policies, but not a geo-mashup generated by individual creators that have no connection to the BNP who therefore have different levels of understanding about the privacy requirements of rank-and-file BNP members. Even if individual privacy preferences had travelled with the data as meta-data tags, as Zittrain suggests, there is no suggestion in the BNP scenario that the ultimate geo-mashup creators would have respected those preferences, especially the creators of the BNP Proximity Search geo-mashup.

The author contends that even if a privacy preference network such as that highlighted by Warner and Chun[299] had been in place with the BNP, it would have had little practical effect on the creation of geo-mashups. The reason being, as highlighted by Zittrain, is that privacy protection is still based on the regulation of data collection organizations and on limited and identifiable information provision and use pathways.[300] As highlighted above, the pathways involved in the BNP geo-mashup were numerous, were more socially complex, and were not identifiable until they were created.

At this point, it is important to acknowledge that the privacy problem that emerged from the BNP geo-mashup is possibly an extreme example because it involved a socially sensitive situation. These sensitivities were exacerbated because the geo-mashup creators used a combination of sensitive and personal information that was aggregated by residential address. However, the issues raised by this example are equally applicable to less socially charged and

[298] *Id*. at 84.

[299] *See id.* at 88–89 (summarizing Warner and Chun's privacy preference network proposal, and their hopes for its applications).

[300] Zittrain, *Privacy 2.0*, *supra* note 147, at 68.

sensitive situations due to the involvement of individual geo-mashup creators rather than organizations. The BNP geo-mashup situation brings Privacy 2.0 issues closer to the fore because of the disgruntled employee's data breach, which effectively severed any possibility that individual BNP members could have a say in how their personal information was subsequently re-used. The same principles arise in other Web 2.0 personal information collection and use scenarios, such as the collection of personal information by individuals as human sensors, or the exchange of personal information in the inchoate data collectives highlighted above. The real issue of significance is the social, temporal, and cultural distance between the provision or collection of personal information by individuals and the re-use of that information in geo-mashup form. It is this distance that can give rise to unresponsive or uncaring re-uses of personal information that have the potential to infringe privacy without the prospect of any real accountability. Whether extensive use of privacy conscious meta-data tags can bridge this distance remains to be seen.

Where then do technical solutions for privacy invasive geo-mashups arise if not through the creation and instigation of more complex privacy policy networks and meta-data tags? One possible solution could reside with geo-browsers themselves. Geo-browsers could inhibit access to residential address aggregation, particularly when large numbers of residential addresses are involved. Large-scale aggregation would therefore only be possible at a zip code, town, or state level rather than at the individual residential address level. This would provide a level of anonymity in the form of broad rather than specific location which would restrict the situations from which an individual could be identified. Accordingly, it would simply not be technically possible for a geo-mashup creator to create maps based on the aggregation of multiple residential addresses. It would still be possible to create a geo-mashup based on an individual tag that relates to an individual residential address, but it would not be possible to aggregate and overlay hundreds or thousands of records over numerous residential addresses. A solution of this type will not prevent all privacy problems. However, the blocking of residential address aggregation would ensure that similar problems to those generated by the BNP geo-mashup are not repeated. Whilst the BNP membership list may still be available on the Internet via Bit Torrent websites, the elimination of mass aggregation using residential addresses at least reduces the scope for privacy invasive activities arising from the use of online mapping applications.[301]

A number of issues could arise from the suggested approach. Firstly, it would require geo-browsers to identify residential properties on their mapping systems. This, in itself, is likely to be a complex and potentially expensive exercise. Secondly, restricting aggregation access to residential addresses could stifle the legitimate innovations of non-privacy invasive geo-mashups like, for example, Housingmaps.com. A potential solution for the second issue

[301] The author acknowledges that it would be possible for an individual or an organization to undertake individual tagging of addresses in similar scenarios but at least that would take time to complete and the time taking would in itself provide some form of limited protection.

may lie in a reverse approach to the publication of My Maps. Instead of a default setting that allows anyone to aggregate anything onto any map, aggregation access to numerous residential addresses would be restricted to those individuals or corporate entities who are willing to enter into a license agreement with geo-browsers that sets boundaries relating to the aggregation of information with residential addresses. The author acknowledges that such a licensing arrangement would still be open to potential abuses, but it would be at least a first step on a journey to provide effective privacy protections against privacy invasive geo-mashups. Moreover, a licensing arrangement may assist with the development of standards relating to good privacy practices in geo-mashups. However, it is clear that further research is required to investigate the feasibility of any long-term technical or legal solution.

B. Social Standards

Technical solutions inherently come packaged with social standards that enable and foster good uses of technology. In *Privacy 2.0*, Zittrain states that the development of social tools, in the form of code-backed norms, is of equal importance as technical solutions to the effective regulation of privacy protections regarding the generative Web.[302] He contends that "a simple, basic standard created by people of good faith can go a long way toward resolving or forestalling a problem containing strong ethical or legal dimensions."[303]

Public and private sector organizations have developed corporate standards for the use of Web 2.0 technologies, particularly social networking sites. For example, the British Broadcasting Corporation (BBC) has devised a set of principles for their staff to follow when using Web 2.0 Internet applications in areas where conflicts can arise.[304] The guidelines and their principles are designed to primarily protect the interests of the Corporation but they nonetheless attempt to raise awareness of privacy issues and to set standards for individual participation on the Internet. For instance:

> Social networking sites provide a great way for people to maintain contact with friends. However, through the open nature of such sites, it is also possible for third parties to collate vast amounts of information.
>
> . . . .
>
> All BBC staff should be mindful of the information they disclose on social networking sites. Where they associate themselves with the Corporation (through providing work details or joining a BBC network) they should act in a manner which does not bring the BBC into disrepute.

[302] *See* Zittrain, *Privacy 2.0*, *supra* note 147, at 118 (discussing the importance of code-backed norms to protect privacy.

[303] *Id*. at 104.

[304] British Broadcasting Corporation, Guidance Note: Personal Use of Social Networking and Other Third Party Websites (Including Blogging and Personal Web-Space), http://www.bbc.co.uk/guidelines/editorialguidelines/assets/advice/personalweb.pdf (last visited Nov. 22, 2009).

> . . . .
>
> Under no circumstance should offensive comments be made about BBC colleagues on the Internet. This may amount to cyber-bullying and could be deemed a disciplinary offence.
>
> . . . .
>
> Personal blogs and websites should not be used to attack or abuse colleagues. Staff members should respect the privacy and the feelings of others. Remember also that if they break the law on a blog (for example by posting something defamatory), they will be personally responsible.[305]

IBM[306] and the Australian Public Service Commission have released similar standards.[307] At the privacy regulator level, both the UK's Information Commissioner[308] and the Australian Office of the Privacy Commissioner[309] have released information about the safe use of personal information on social networking sites. A conglomeration of major media and software commercial copyright owners has also developed the Principles for User Generated Content (UGC) Services, which seek "to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners."[310] The purpose of the UGC Principles is to eliminate user-generated material that infringes copyright while encouraging the uploading of legitimate content and the protection of legitimate interests of user privacy.[311] However, none of these fledgling standard setters provides guidance on the creation and use of geo-mashups, either at a corporate or individual level.

The BNP geo-mashup example shows that there is already an awareness of privacy issues arising from the use of personal information amongst geo-mashup creators. For example, three of the four geo-mashups noted, namely the *Times*, the *Guardian* and the BNP Near Me geo-mashup, did not publish

[305] *Id*. at 2–5.

[306] IBM, IBM Social Computing Guidelines: Blogs, Wikis, Social Networks, Virtual Worlds and Social Media, http://www.ibm.com/blogs/zz/en/guidelines.html (last visited Nov. 22, 2009).

[307] Australian Public Service Commission, Circular 2008/8: Interim Protocols for Online Media Participation, http://apsc.gov.au/circulars/circular088.htm (last visited May 19, 2009).

[308] Information Commissioner's Office, Using Social Networking Sites Safely (Nov. 23, 2007), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/social_networking_v04_final.pdf.

[309] Office of the Privacy Commissioner, Your Privacy Rights FAQ, http://www.privacy.gov.au/faq/individuals#social_networking (last visited Feb. 19, 2010).

[310] UGC Principles, Principles for User Generated Content Services, http://www.ugcprinciples.com/ (last visited Feb. 19, 2010).

[311] The UGC Principles have a limited consideration of privacy protection issues for individuals, and focus mainly on protecting the interests of copyright holders. For instance, Principle 10 states:

> Consistent with applicable laws, including those directed to user privacy, UGC Services should retain for at least 60 days: (a) information related to user uploads of audio and video content to their services, including Internet Protocol addresses and time and date information for uploaded content; and (b) user-uploaded content that has been on their services but has been subsequently removed following a notice of infringement. UGC Services should provide that information and content to Copyright Owners as required by any valid process and consistent with applicable law.

Id.

any BNP related personal information. Moreover, these geo-mashups aggregated their maps around postcodes rather than individual residential addresses. By doing so, they provided a degree of privacy protection by obscuring the identity of residential addresses that are linkable to BNP members. Concerns still arose, however, because of the particular nature of UK postcodes and their effect when aggregated with Google Maps. The BNP Near Me geo-mashup creator altered his original geo-mashup because its pinpoints gave a misleading impression that a BNP member resided at a specific address when in fact the representation of the BNP membership data was incorrect. The creator of the geo-mashup explained his reason for changing and ultimately removing the geo-mashup from the Internet.

> I have decided to take down the map. Many people have commented that the map does give a false impression of accuracy, despite my making this clear, and I'm tempted to agree. I do not want to single anybody out and by removing the accuracy from the map it is possible that it ends up incorrectly implying a property contains a BNP member. It has been suggested that an inaccurate map that doesn't make that clear is worse than publishing the list itself, and I think that's a reasonable comment.[312]

There is a clear recognition of the negative consequences that could arise from the use of inaccurate personal information that could give a misleading impression. Owad also highlighted similar concerns in the Amazon wish list geo-mashup.[313] However, the opposite occurred with the BNP Proximity Search geo-mashup, which provided the postcodes and names of BNP members, and then overlaid that information over specific residential addresses.[314] The Proximity Search geo-mashup may or may not have been aggregated on an individual address or a postcode. However, it is possible to

[312] Butcher, *Updated: BNP Member List*, *supra* note 96.

[313] As Owad noted in his article:

> Thanks to Google Maps (and many similar services) a street address is all we need to get a satellite image of a person's home. Tempted as I was to provide satellite images of the homes of the search subjects, it just seemed a bit extreme even for this article. Instead, I opted only to pinpoint the centers of the towns in which they live. So at least you'll know that there's *somebody* in your community reading Critical Thinking or some other dangerous text.

Owad, *supra* note 101.

[314] Similar criticisms can also be raised relating to the Gawker staff, who seem acutely unaware of the privacy issues arising from Gawker Stalker. *See Larry King Live: Paparazzi: Do They Go Too Far?* (CNN television broadcast Apr. 6, 2007), *transcript at* http://transcripts.cnn.com/TRANSCRIPTS/0704/06/lkl.01.html, *video excerpt at* http://www.youtube.com/watch?v=2-avakrRUaU (documenting Jimmy Kimmel's interview with Emily Gould, the then-editor of Gawker, on *Larry King Live*). One Gawker editor described the Gawker staff's reactions to criticism of the site:

> But Gawker editors were "totally taken aback by the big whole to-do" over the maps, says one of them, Jesse Oxfeld. "We thought we were using a cool new tool, adding a new element" that didn't provide additional information. Stalker sightings, which have always come with a none-of-this-is-verified disclaimer, have typically included specifics; it's just that now they're presented in both visual and text form.
>
> The uproar was "hysterical," Oxfeld says. "We had *Access Hollywood* saying we're destroying celebrity lives." And since the maps—and the PR mayhem—started, sightings have increased, he says.

Freydkin & Barker, *supra* note 153.

use the geo-mashup to identify a BNP member at a specific street, because (a) it is possible to reverse search a postcode to find a corresponding street address, which can be cross referenced with other sources to check where a particular person lives; or (b) that person does in fact reside at that address, which, again, can be confirmed with a relatively quick check of other data sources. As such, the author contends that the BNP Proximity Search has infringed expected social standards regarding the use of personal and non-personal information in geo-mashups as exemplified by the actions of the other BNP geo-mashup creators.

At this point Zittrain's contentions regarding the establishment of code-backed norms as a means of privacy protection look a trifle weak. The BNP Proximity Search geo-mashup gives rise to serious privacy concerns and yet the geo-mashup is still available on the Internet. At what point does further action need to be taken either to remove the geo-mashup or to ensure that access is restricted? Either solution is potentially difficult to implement because the BNP membership list has been widely disseminated and neither solution guarantees that the same problem would not arise again. What code-backed norms can do, however, is to provide a spotlight for those geo-mashups that can give rise to privacy invasive tendencies, enabling earlier identification by individuals, organizations, or geo-browsers before more serious problems emerge from publication via the blogosphere or via the ubiquity of search engines.

The technical solution, highlighted above, would mitigate the threats of privacy invasive geo-mashups and would require geo-browsers to restrict aggregation and overlay of information on individual residential addresses. The author does not intend to single out geo-browsers as the new pseudo-regulators of privacy in geo-mashups, but it nonetheless needs to be acknowledged that these organizations are the gatekeepers for geo-mashup creation because they facilitate the geo-mashup process with their technologies. As such, it is no longer sufficient for geo-browsers to provide only one means of remedial relief for individuals against privacy invasive geo-mashups in the form of simple take down notices. Proactive standard setting is now required to augment reactive removal of privacy infringing material.

As a first step, this article suggests that the major geo-browsers work together with the geospatial community, privacy regulators, and reputed privacy organizations to develop a new set of privacy-oriented standards for the creation of geo-mashups, in order to increase awareness of the detrimental issues that can arise from privacy invasive geo-mashups. These privacy standards for geo-mashups could be the first step in a continuing evolution of social norm development that (a) sets standards for the collection and use of personal information in the creation of geo-mashups, and (b) allows a flexible framework in which individual concerns, geo-mashup creator innovations, and geo-browser requirements can be aired and discussed. Part of this ongoing societal discussion will also need to address interaction with existing and future legal frameworks.

C. Legal Frameworks

The essence of Zittrain's work is the development of "bottom-up" initiatives[315] to counteract the weaknesses of existing privacy laws that simply fail to cope with the complexities of online personal information exchange. However, embedded social and technical solutions, which have no recourse to legal frameworks, inherently rely on self-regulatory measures for enforcement and remedies. During the last decade, there has been voluble criticism regarding the self-regulation of privacy protections.[316] The main criticism being that there is an overwhelming incentive for private sector data collecting organizations to breach, rather than preserve, privacy protections.[317] As such, critics argue that standalone self-regulatory measures, with no recourse to underlying legal frameworks, do not provide effective privacy protections.[318] After an extensive review of international privacy protection instruments, Bennett and Raab produced four sets of factors that indicate where a self-regulatory environment for privacy protections is likely to be adopted and is more likely to be effective.[319] First, organizations that conduct operations at an international level are exposed to a greater level of international privacy standards, and a higher motivation exists to adopt self-regulatory practices to comply with those standards. Second, the introduction of new technologies, which have publicly perceived privacy implications, provide a motive for self-regulation that attempts to anticipate problems before they occur and thus assures consumers that their privacy is not at risk. Third, situations involving actual or potential negative publicity also provide an impetus. Finally, industry structure can have an impact on the introduction of self-regulatory measures, especially if there is a broadly representative trade association that can self-regulate the industry.

A brief overview of Bennett and Raab's work shows that the conditions for effective self-regulation heavily entail the notions of first generation information privacy laws that protect individuals from data collecting organizations—albeit protections governed by the organizations themselves. As highlighted above, many of the concerns that arise from privacy invasive geo-mashups are generated by individuals rather than organizations. At the

[315] One of Zittrain's articulations of this idea follows:

> Enduring solutions to the new generation of privacy problems brought about by the generative internet will have as their touchstone tools of connection and accountability among the people who produce, transform, and consume personal information and expression: tools to bring about social systems to match the power of the technical one.

Zittrain, *Privacy 2.0*, *supra* note 147, at 118.

[316] *See, e.g.*, Roger Clarke, *Privacy as a Means of Engendering Trust in Cyberspace Commerce*, 24 U.N.S.W. L.J. 290, 295 (2001) [hereinafter Clarke, *Cyberspace Commerce*] ("Self-regulation is seen by the public for what it is: supervision of the sheep by the wolves, for the benefit of the wolves, and a means for business to establish a pretence of regulation in order to hold off actual regulation."); Hoofnagle, *Privacy Self-Regulation*, *supra* note 260 (reviewing self-regulatory failures involving privacy in the United States); *see also* BENNETT & RAAB, *supra* note 216, at 171 (summarizing critics of self-regulation).

[317] BENNETT & RAAB, *supra* note 216.

[318] Clarke, *Cyberspace Commerce*, *supra* note 316, at 295–97.

[319] BENNETT & RAAB, *supra* note 216, at 172–73.

same time, it is clear that informal social standards are in existence regarding the appropriate use of personal information in geo-mashups as evidenced by the different BNP geo-mashups and the awareness that pinpointing information to residential addresses can give rise to privacy concerns. So where does the balance lie, both in terms of Privacy 2.0 and the governance of protections relating to privacy invasive geo-mashups, between the instigation of "bottom-up" social and technical standards generated by Internet users and geo-browsers, and the "top-down" legal sanctions of first generation laws applied by privacy regulators and the courts?

Zittrain's analysis of first generation privacy laws is persuasive because it vividly highlights the limits of these laws against new technological and social initiatives arising from the Internet. Moreover, the recognition that legal, social, and technical developments are derived from the interaction of many different sources provides a healthy impetus to enhance discourse about appropriate uses of personal information in geo-mashups specifically, and in society in general. However, technical solutions and socially developed standards for privacy protection must be embedded in a legal framework in order to provide effective privacy protections. A technical solution or a socially developed standard should assist and inform the development of legal privacy protections but they should not be a substitute for those protections.

It is beyond the scope of this article to define an appropriate Privacy 2.0-based legal framework for geo-mashups, but it is apparent from Zittrain's analysis and the examples provided above, that we have entered a time when the parameters of online personal information usage are getting manifestly broader while the scope of first generation information privacy laws are getting increasingly narrower. The death knell for first generation privacy laws may or may not be sounding—it is too early to say, and it is a matter of such importance that to suggest so, without recourse to extensive policy, legal, and social analysis, would be giving lip service to a complex concern and an essentially contested social issue. That said, a more appropriate balance needs to be sought between "bottom-up" activities and "top-down" directions that recognizes the value that each brings to the regulation of privacy and the legal protections afforded. The former can augment the latter, but it is the latter that sets the standards to be augmented by the former. This process of continual augmentation will be characterized by the balance or imbalance of interaction between all parties involved in the creation, publication, and direct or indirect regulation of Internet activities, including geo-mashups. In that regard, it is hoped that Zittrain's call for a wider social discourse about the regulation of privacy will be the most enduring aspect of his Privacy 2.0 analysis.

VII. CONCLUSION

This article has highlighted the privacy concerns that can arise from privacy invasive geo-mashups particularly in light of the limits of first generation information privacy laws as suggested by Zittrain. The Internet now provides manifold pathways for the provision and use of personal information providing numerous Internet users, with multiple opportunities to use personal information in many different ways. More importantly, in terms of information privacy regulation, these multiple users can be individuals as well as organizations. Potential Privacy 2.0 solutions for the prevention and mitigation of privacy problems reside in the development of embedded technical and social standards, and not solely through avenues of legal recourse founded on the concept of information privacy. These standards, by their nature, must be inclusive and flexible given the changes that are taking place in the everyday Web 2.0 environment. Moreover, whilst the article acknowledges the limits of first generation information privacy laws with regard to Web 2.0 environments, including geo-mashups, it is too early to say whether we are witnessing the death of first generation information privacy laws in general. First generation laws may still have a place regarding the regulation of interaction between individuals and organizations about the provision and re-use of personal information along more traditional lines involving stable information collection relationships and defined information pathways. Privacy 2.0 requirements suggest a move from laws based purely on information privacy to the establishment of laws, codes, and norms that reflect, and respect, the conceptual complexity and uncertainty of privacy, which is fitting for ever-changing online environments. This article has put forward legal, organizational, technical, and social solutions in the form of standard development that would help to alleviate some of the concerns arising from privacy invasive geo-mashups. The author hopes that geo-browsers take up the call for the development of privacy standards for geo-mashups, which will assist with the complex balancing act of encouraging further geo-mashup innovations, whilst at the same time enshrining acceptable uses of personal information that will assist courts and privacy regulators to identify and respond to privacy infringements arising from privacy invasive geo-mashups.