Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

خصوصية البحث على الإنترنت

د. فايزة دسوقي أحمد
مدرس، قسم المكتبات والوثائق
كلية الآداب – جامعة بني سويف، مصر
أستاذ علم المكتبات والمعلومات المساعد
قسم دراسات المعلومات
جامعة الإمام محمد بن سعود الإسلامية

المستخلص:
تهدف الدراسة إلى معرفة مدى مراعاة محركات البحث لخصوصية المستخدمين، وكذلك تقديم الاقتراحات التي يمكن من خلالها المساعدة في حماية خصوصية المستخدمين أثناء بحثهم على الإنترنت. ومن أهم النتائج التي توصلت إليها، أن محركات البحث تجمع كم هائل من المعلومات عن المستخدمين، وأن من السهل جدًا عليها تحديد هوية مستخدم معين، إذا كان مُسجلا فيها، أو اشترى شيئًا أثناء تواجده على موقعها. وأن هناك الكثير من المخاطر قد تقع نتيجة جمع هذه المعلومات. ويمكن للمحركات أن تتشارك في المعلومات التي تجمعها من المستخدمين أو عنهم مع جهات أخرى، دون موافقة المستخدم. ولا تتيح غالبية المحركات للمستخدم، إمكانية حذف بيانات بحثه من خوادمها. ويمكن إجمال هذه النتائج في أن: غالبية محركات البحث لا تحافظ على خصوصية البحث للمستخدم؛ فهي لا تتيح له الفرصة لتحديد المعلومات التي ستُجمَعُ منه أو عنه، كما أنها تكشف عن هذه المعلومات لأطراف أخرى دون موافقة منه.

الاستشهاد المرجعي بالبحث
فايزة دسوقي أحمد. خصوصية البحث على الإنترنت .- cybrarians journal .- ع 18 (مارس 2009) . - تاريخ الاتاحة < اكتب هنا تاريخ اطلاعك على الصفحة > . - متاح في :<أكتب هنا رابط الصفحة الحالية>

1/1 المقدمة:

تهتم الخصوصية Privacy بحق الفرد في تحديد المعلومات التي ستُجمَعُ منه أو عنه، وحقه في عدم اطلاع الآخرين عليها دون موافقة منه. وتساعد الخصوصية في الحفاظ على صحة الفرد النفسية، فتنتهك حرية الشخص وكرامته واستقلاليته عندما تُنتهك خصوصيته. فعندما يعلم القارئ –على سبيل المثال- أن ما يقرأه مُراقب، فقد يقوم بنوع من

الرقابة الذاتية، مما يجعله لا يقرأ ما يريد حتى لا يعطي فرصة للآخرين لمعرفة آرائه واتجاهاته. لذا يمكن القول بأن انتهاك الخصوصية مثل الرقابة، يهدد الحرية الفكرية (Oppenheim and Natalie 2000).

وقضايا خصوصية الأفراد على الإنترنت من القضايا الشائكة في العصر الحالي؛ حيث يمكن أن تشكل الإنترنت تهديدًا للخصوصية. وينشأ هذا التهديد عن عدد من العوامل، منها: أن منتجات الإنترنت غالبًا ما تنطوي على الحاجة إلى تسجيل الفرد، ويؤدي هذا التسجيل إلى زيادة الكشف عن المعلومات الشخصية من جانب المستهلكين، مما يتيح للشركات على الإنترنت عملية الاستيلاء على البيانات. كما تسمح التقنيات الجديدة بالتعرف على المستخدمين، والاستيلاء على مستويات تفصيلية متزايدة من المعلومات عنهم (Privacy International, 2007)، كما وفرت تلك التقنيات نظمًا يمكنها اعتراض الرسائل الإلكترونية للأشخاص، ونظمًا أخرى يمكنها تتبع أبحاثهم؛ ... (Hinman, 2005).

ولعل من أطرف ما قيل في وصف الوضع الحالي لخصوصية الفرد على الإنترنت ما ذكره Duberman و Beaudet من أنه "قد يكون من الصحيح على الإنترنت في السابق، أن أحدًا لن يعرف أنك كلب - كما جاء في فيلم كرتوني قديم- ولكن كما يقولون الآن على الشبكة، فإنه من الممكن أن يعرف المسوقون العلامة التجارية التي تفضلها لطعام الكلاب، حيث من المحتمل أن تكون قد عرفت نفسك لهم [عند شراء طعام كلبك منهم]"! (Duberman and Beaudet, 2000)

2/1 التعريفات الإجرائية:

المصطلحان الأساسيان في الدراسة الحالية هما:

1. خصوصية البحث Search privacy : حق المستخدم في تحديد المعلومات التي ستُجمع منه أو عنه أثناء بحثه على الإنترنت، وحقه في الحفاظ على سرية تلك المعلومات، وعدم إفشائها لأطراف أخرى دون موافقة منه.

2. المستخدم User: الشخص الذي يجري أبحاثه على الإنترنت.

3/1 موضوع الدراسة وأهميته:

تتنوع الخدمات المقدمة عن طريق الإنترنت، فهناك خدمة إجراء الأبحاث، وخدمة البريد الإلكتروني، وخدمة المحادثة Chat، وخدمة التسوق، وغير ذلك من الخدمات. وتجلب كل خدمة من هذه الخدمات، قضايا متنوعة تتعلق بخصوصية الأفراد الذين يستخدمونها. ولعل خدمة البحث من أهم تلك الخدمات، ومحركات البحث هي مفتاح الفضاء المعلوماتي cyberspace لإيجاد المعلومات المطلوبة على الإنترنت، لذا هي أداة لا غنى عنها للأفراد، مما جعل من المهم والضروري التعرف عن كثب عما يجلبه استخدام تلك المحركات من قضايا تتعلق بخصوصية الأفراد.

وتتمثل أهمية الدراسة الحالية في رصد وتحليل ممارسات محركات البحث فيما يتعلق بخصوصية الأبحاث التي تُجــرى من خلالها على الإنترنت، وما يمكن أن تمثله تلك الممارسات من خطورة على المستخدمين.

4/1 أهداف الدراسة:

تهدف الدراسة إلى معرفة مدى مراعاة محركات البحث لخصوصية المستخدمين، وكذلك تقديم الاقتراحات التي يمكن من خلالها المساعدة في حماية خصوصية المستخدمين أثناء بحثهم على الإنترنت.

5/1 تساؤلات الدراسة:

تتمثل التساؤلات التي تحاول الدراسة الإجابة عنها، فيما يلي:

- ما أنواع المعلومات التي تجمعها محركات البحث عن المستخدمين؟
- ما المخاوف من جمع محركات البحث لبيانات المستخدمين؟
- ما أساليب جمع محركات البحث لبيانات المستخدمين؟
- ما أسباب جمع محركات البحث لبيانات المستخدمين؟
- ما فترات احتفاظ المحركات ببيانات البحث؟
- كيفية حذف المحركات لبيانات البحث؟
- هل تشارك المحركات بيانات البحث مع جهات أخرى، وهل تأخذ موافقة المستخدم على ذلك؟
- هل تسمح محركات البحث للمستخدمين بالوصول إلى بيانات أبحاثهم وحذفها؟
- ما الطرق المقترحة لحماية خصوصية البحث على الإنترنت؟

6/1 عينة الدراسة:

تم اختيار محركات البحث العامة الخمسة الأكثر استخدامًا علــى الإنترنــت، وهــي: Google، و Yahoo، و Ask، و AOL (من خلال محرك بحثه AOL Search) ، و MSN (من خــلال محــرك بحثــه Live Search)(Center for Democracy Technology, 2007)، كعينة للاسترشاد بها في التعرف إلــى ممارســات محركــات البحــث بالنســبة لخصوصية البحث، وذلك من خلال تحليل ما جاء في تصريحاتها وسياسات الخصوصية بها، ومــا أُعــد عنهــا مــن دراسات. ويبين الجدول رقم (1) موقع هذه المحركات على الإنترنت.

الجدول رقم (1)

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

مواقع محركات البحث عينة الدراسة على الإنترنت (*)

م	محرك البحث	الموقع على الإنترنت
1	AOL Search	http://search.aol.com/
2	Ask	http://www.ask.com/
3	Google	http://google.com/
4	Live Search	http://www.live.com/
5	Yahoo	http://www.yahoo.com/

(*) تم ترتيب المحركات هجائيًا.

7/1 حدود الدراسة:

1/7/1 الحدود الموضوعية:

تتناول الدراسة موضوع خصوصية البحث على الإنترنت، بغض النظر عن موضوع البحث.

2/7/1 الحدود النوعية:

تقتصر الدراسة على خصوصية البحث على الإنترنت، باستخدام محركات البحث العامة.

3/7/1 الحدود اللغوية:

تغطي الدراسة خصوصية البحث على الإنترنت، باستخدام محركات البحث العامة التي تبحث باللغة الإنجليزية واللغات الأخرى.

4/7/1 الحدود الزمنية:

تغطي الدراسة ممارسات محركات البحث العامة فيما يتعلق بخصوصية البحث حتى ديسمبر 2008م.

8/1 منهج البحث وأدواته:

استخدمت الباحثة في هذه الدراسة المنهج الوصفي التحليلي، وذلك لرصد ممارسات محركات البحث فيما يتعلق بخصوصية الأبحاث وتحليلها، لمعرفة مدى مراعاة تلك المحركات لخصوصية المستخدمين.

وقد تنوعت الأدوات التي اعتمدت عليها الدراسة؛ حيث تم استخدام "سياسات الخصوصية" في محركات البحث الخمسة السابق ذكرها، لمعرفة ما تنص عليه فيما يتعلق بخصوصية البحث. وكذلك "القراءات النظرية" للعديد من الدراسات التي تناولت هذا الموضوع. بالإضافة إلى "الملاحظة" التي أُستخدمت عند البحث في العديد من المحركات، وتقييم ممارساتها فيما يتعلق بخصوصية البحث، لتحديد أكثرها مراعاة لخصوصية المستخدمين.

9/1 الدراسات السابقة:

تبين من استعراض الباحثة لما تم من دراسات عربية وأجنبية في الأدلة والببليوجرافيات التي ترصد الإنتاج الفكري في مجال المكتبات والمعلومات، وجود ندرة في الإنتاج الفكري العربي في موضوع خصوصية البحث على الإنترنت، حيث لا توجد دراسة عربية تتعلق بهذا الموضوع –على حد علم الباحثة- باستثناء الدراسة التي أعدتها في نهاية عام 2008م. هدفت من خلالها تحليل سياسات الخصوصية العامة في عينة من محركات البحث العربية والأجنبية، لاستكشاف القضايا التي عالجتها المحركات في تلك السياسات. ومن أهم النتائج التي توصلت إليها الدراسة أن محركات البحث لديها القدرة على جمع كم هائل من المعلومات عن مستخدميها، ويمكنها دمج المعلومات التي يتم جمعها عن المستخدم في ملف واحد، وتتنوع الأسباب التي تقف وراء جمع محركات البحث للمعلومات عن المستخدمين، وتشارك محركات البحث معلومات المستخدمين مع أطراف أخرى في عدة حالات، ولم تراع السياسات الحد الأدنى من المعايير التي وضعها قانون حماية خصوصية الأطفال على الإنترنت، وأن سياسات الخصوصية في محركات البحث العربية أضعف بكثير من نظيراتها في المحركات الأجنبية (أحمد، قيد النشر). ومن الواضح أن هذه الدراسة لم تهدف إلى دراسة خصوصية البحث، وإنما هدفت إلى معرفة القضايا التي عالجتها سياسات الخصوصية في محركات البحث.

أما الدراسات الأجنبية، فقد تناول العديد منها موضوع خصوصية البحث على الإنترنت باستخدام محركات البحث، ومن أهمها:

الدراسة التي أُجريت من قِبل Pew Internet & American Life Project في عام 2004م، على عينة مكونة من 2,200 أمريكي من البالغين الذين تبلغ أعمارهم 18 عامًا فأكثر، وهدفت إلى تعرف ملامح الاستخدام اليومي للإنترنت من قبل الأمريكيين، وذلك من خلال معرفة مدى اعتمادهم على محركات البحث وثقتهم بها، ورضاهم عن النتائج التي توصلوا إليها. ومدى إدراكهم لكيفية إنجاز المحرك لأبحاثهم، وتقديمه للنتائج. وقدمت الدراسة عددًا من النتائج، ما يهمنا منها في البحث الحالي، النتائج المتعلقة بخصوصية البحث، التي بينت أن (43%) من المبحوثين ذكروا أنهم على علم بقضايا تعقب محركات البحث للمستخدمين، بينما (57%) لا يعلمون بذلك. وأن (37%) من المبحوثين يوافقون على هذه الممارسات بصفة عامة، بينما (55%) يرفضونها. وأن (51%) من المعترضين، ذكروا أنهم قد يغيرون رأيهم،

ويوافقون على تعقب محرك البحث لأنشطتهم، إذا بين المحرك بوضوح ممارساته للمستخدمين، بينما استمر (44%) على رفضهم. وذكر (67%) من النسبة التي استمرت على الرفض، أنهم سيتوقفون عن استخدام محرك البحث إذا علموا أنه يتعقب أبحاثهم. ويعني هذا أن (21%) من مستخدمي الإنترنت سيتوقفون عن استخدام محرك البحث إذا علموا أنه يتعقب أبحاثهم (Fallows, 2005). ومن الواضح أن هذه الدراسة، لم تركز على خصوصية البحث فقط، بل تناولت قضايا متنوعة أخرى، كما أنها لم تدرس ممارسات محركات البحث للتعرف إلى كيفية معالجتهم لخصوصية المستخدمين، بل أجرت دراسة ميدانية على الأشخاص الذين يستخدمون محركات البحث، بالإضافة إلى أنها لم تقدم أية توصيات أو مقترحات تساعد المستخدمين في الحفاظ على خصوصية أبحاثهم.

كما وجه Elinor Mills و Declan McCullagh المحرران في CNET News عام 2006م، سبعة أسئلة إلى أكبر أربع شركات بحثية هيAmerica Online، وGoogle، وMicrosoft، وYahoo؛ لاكتشاف أنواع المعلومات التي يحتفظون بها عن مستخدميهم، ومدى تخزين عنوان بروتوكول الإنترنت مرتبطًا مع مصطلحات البحث ونوعه. ومدى إمكانية إعداد قائمة بالأفراد الذين بحثوا بمصطلح معين، من خلال عنوان بروتوكول الإنترنت الخاص بهم أو قيمة ملف تعريف الارتباط، ومعلومات أخرى تتعلق بحفظ البيانات عن أبحاث المستخدمين، وما إذا كان المحرك يتيح للمستخدمين طريقة لحذف تلك البيانات.... والمحرران لم يقوما بتحليل الإجابات للخروج بنتائج مقارنة، بل ذكرا فقط ما ذكره المتحدث باسم كل شركة حرفيًا وبشكل منفصل (McCullagh and Mills, 2006).
وفي أغسطس من العام التالي وجه نفس المحررين، ثمانية أسئلة إلى أكبر شركات تقود عمليات البحث (Google، وYahoo، وMicrosoft، وAsk ، وAOL)، منها: ما طول المدة التي يحتفظون فيها بالبيانات، وكيف يتخلصون منها في النهاية، وإذا ما كانوا مرتبطين بتوجيه السلوك، وما إذا كانوا يستخدمون المعلومات التي جمعوها من المستخدمين لتوجيه الإعلانات المعروضة. وقد تبين من مقارنة الإجابات أن Ask هي أكثر الشركات حماية لخصوصية المستخدم. كما تبين أن تلك الشركات أدخلت تحسينات على فترة احتفاظهم بالبيانات، مقارنة بالدراسة السابقة (McCullagh and Mills, 2007).

وفي عام 2007م أعد Center for Democracy Technology تقريرًا قارن فيه بين ممارسات الخصوصية في أكبر محركات البحث (Google، وYahoo، وMicrosoft، وAsk.com ، وAOL) وفقًا لما جاء في سياسات الخصوصية بها، وما أعلنوه في تصريحاتهم حول العناصر التالية: الفترة الزمنية التي يتم الاحتفاظ فيها ببيانات الأبحاث التي يجريها الباحثون، وكيفية حذف تلك البيانات والتخلص منها، ومدى مشاركة معظم أو كل بيانات البحث مع أطراف ثالثة على أساس مستمر (Center for Democracy Technology, 2007). وقدم التقرير العديد من التوصيات، إلا أنها كانت توصيات نظرية ولم تتطرق لخطوات عملية يمكن للمستخدم من خلال تطبيقها الحفاظ على خصوصية بحثه.

وفي العام نفسه، أُعِدَّ تقريرٌ هدف إلى مساعدة المستهلكين؛ حتى يتمكنوا من اتخاذ القرار المتعلق بتحديد الشركات التي سيستخدمونها على الإنترنت. وإعلام الشركات أن ممارساتهم وأنشطتهم مراقبة. واشتملت الدراسة على أهم شركات خدمات الإنترنت، التي تم تحديدها وفقًا لحجم الحصة من السوق، والخدمات المقدمة، وعدد المستخدمين، وهي: Amazon ، و AOL ، و Apple ، وBBC ، و Bebo ، وeBay، و Facebook، وFriendster ، و Google ، و Hi5، و Last.fm ، وLinkedIn ، وLiveJournal ، و Microsoft ، وMyspace ،و Orkut، و Reunion.com، و Skype، وXanga Wikipedia ، وWindows Live Space ، وYahoo! ، و YouTube. وقد تناول التقرير التفاصيل الإدارية للشركات، لمعرفة ما إذا كانت الشركة لديها إدارة أو شخص مسؤول عن الخصوصية، وأنواع المعلومات التي تُجمع في الموقع، بالحصول على موافقة الشخص أو بدونها، ومدة الإبقاء على تلك المعلومات، والانفتاح والشفافية في الموقع عن إعلان ممارساته فيما يتعلق بخصوصية المستهلكين. وكيفية استجابة الشركة لشكاوى المستهلكين المتعلقة بالخصوصية، وما إذا كانت الشركة تتيح للمستخدمين الوصول إلى معلوماتهم الشخصية وتصحيحها، وكيفية التعامل مع الطلبات المقدمة من وكالات إنفاذ القانون والحكومات الأجنبية. وتم ترتيب الشركات التي تم دراستها، وفقًا لمدى توافر ومراعاة عوامل حماية الخصوصية، وقد تبين أن Google هي أسوأ شركة في العينة (Privacy International, 2007). ومن الواضح أن التقرير لم يركز فقط على خصوصية البحث، بل على خصوصية الأفراد عند التعامل مع الشركات ومحركات البحث على الإنترنت بصفة عامة.

كما كانت هناك دراسات تناولت الجانب القانوني لخصوصية البحث على الإنترنت، منها: دراسة Jayni Foley، في عام 2007م، التي تناولت قضايا الخصوصية في محركات البحث وموردي خدمة الإنترنت، وبصفة خاصة الخصوصية في Google، بوصفه أكثر محركات البحث استخدامًا. وقد تناولت الدراسة الموضوع من وجهة النظر القانونية فيما يتعلق بشرعية وقانونية طلب الجهات الحكومية من محركات البحث وموردي خدمة الإنترنت الكشف عن السجلات التي تحتفظ فيها ببيانات المستخدمين، من أجل الكشف عن الجرائم ومحاربة الإرهاب. ومن النتائج التي توصلت إليها أن محركات البحث وموردي خدمة الإنترنت لا يوجد لديهم الحافز لتحدي استدعاء الحكومة ورفضه، كما أن التزامها يقل أو ينعدم تجاه إعلام المستخدمين بأن سجلاتهم يتم فحصها (Foley, 2007). كما حللت "pouya bozorgchami" أشهر القضايا المتعلقة بالخصوصية، والمرتبطة بشركات الإنترنت وفقًا لما جاء في التعديل الرابع Fourth Amendment، وأوضحت أن هذا التعديل لا يحمي مصطلحات البحث، كما استعرضت قانون Electronic Communications Privacy Act وبينت أوجه القصور الكامنة فيه. ولم تقتصر الدراسة على خصوصية البحث ومصطلحاته فقط، بل تناولت موضوعات أخرى مثل، خصوصية البريد الإلكتروني (bozorgchami).

ومن الواضح أن الدراسة الحالية تتشابه مع الدراسات السابقة في اهتمامها بقضية خصوصية البحث على الإنترنت. إلا أنها تختلف عنهم في أنها تقدم اقتراحات وخطوات عملية يمكن للمستخدم من خلالها حماية خصوصيته عند البحث على الإنترنت باستخدام محركات البحث، وهو الجانب الذي لم تتناوله أية دراسة منهم.

2. خصوصية البحث في محركات البحث:

يتناول هذا الجزء ممارسات محركات البحث فيما يتعلق بأنواع المعلومات التي تجمعها عن المستخدمين، والمخاوف من جمع تلك المعلومات، وأساليب جمع المعلومات، وأسباب جمع المعلومات، وفترات احتفاظ محركات البحث ببيانات البحث، وكيفية حذف هذه البيانات والتخلص منها، ومدى مشاركة بيانات البحث مع جهات أخرى، وما إذا كانت المحركات تسمح للمستخدمين بالوصول إلى بيانات أبحاثهم وتعديلها.

1/2 أنواع المعلومات التي تجمعها محركات البحث:

تشتمل أنواع المعلومات التي تجمعها محركات البحث (عينة الدراسة)، على:

1/1/2 معلومات عن المستخدم:

تشتمل المعلومات التي تجمعها محركات البحث عن المستخدم، على: الاسم، وعنوان المنزل، وعنوان العمل، ورقم الهاتف، والفاكس، والرمز البريدي، وعنوان البريد الإلكتروني، والعمر، ونوع الجنس، ورقم بطاقة الائتمان (Microsoft, 2008)، ورقم الضمان الاجتماعي، ومعلومات عن الأصول الخاصة، والمهنة، والاهتمامات الشخصية (Yahoo, 2008 d). وتاريخ المنتجات التي تم شراؤها، وعناوين الشحن، والدولة التي يقطن فيها (AOL, 2008 a).

2/1/2 معلومات عن الأجهزة والبرمجيات التي يستعملها المستخدم:

تشتمل المعلومات التي تجمعها محركات البحث عن الأجهزة والبرمجيات التي يستعملها المستخدم، على: نوع المتصفح "على سبيل المثال، Netscape، Internet Explorer" ولغته، ونوع نظام التشغيل "مثل Windows XP أو ماكنتوش Mac OS"، ونوع وحدة المعالجة المركزية "بنتيوم Pentium مثلا"، وطريقة الاتصال بالإنترنت "على سبيل المثال، النطاق الضيق narrowband أو النطاق العريض broadband"، وعنوان بروتوكول الإنترنت (AOL, 2008 a)، والبيانات من أي ملفات تعريف ارتباط غير محذوفة، سبق وأن قبلها متصفح المستخدم من المحرك (Ask, 2008 b) .

3/1/2 معلومات عن الأبحاث التي يجريها المستخدم، وطريقة تصفحه للإنترنت:

تشتمل المعلومات التي تجمعها محركات البحث عن الأبحاث التي يجريها المستخدم، وطريقة تصفحه للإنترنت، على: عنوان الموقع الذي أتى منه المستخدم، والعنوان الذي غادر إليه، ومحرك البحث والكلمات الأساسية التي استعملها للعثور على موقع المحرك، والصفحات التي قام بعرضها ضمن موقع المحرك (Microsoft, 2008). ونص الاستفسار، وتاريخ الطلب ووقته (Google, 2008 b) ، والنتائج المسترجعة التي ضغط عليها المستخدم، واستجاباته للعروض والإعلانات المقدمة من قبل المحرك، وعدد مرات الاستجابة لها (AOL, 2008 a) .

وبالإضافة إلى المعلومات السابق ذكرها، فإن المحرك قد يقوم بتكملة المعلومات التي جمعها، بمعلومات يحصل عليها من شركات أخرى. على سبيل المثال، قد يستخدم خدمات من شركات أخرى تمكنه من تتبع منطقة جغرافية عامة بالاستناد إلى عنوان بروتوكول الإنترنت الخاص بالمستخدم، بغية تخصيص خدمات معينة خاصة بتلك المنطقة الجغرافية(Microsoft, 2008).

ومن الملاحظات التي يمكن الوقوف عليها مما سبق:

- هناك نوعان أساسيان من المعلومات التي يتم جمعها عن المستخدم في محركات البحث، هما: المعلومات الشخصية، والمعلومات غير الشخصية. ويُقصد بـ "المعلومات الشخصية" المعلومات التي يتم جمعها عن شخص ما، وتتيح الاتصال المباشر به. مثل الاسم الأول والأخير، وعنوان المنزل أو العناوين الأخرى مثل اسم الشارع أو المدينة أو البلدة، وعنوان البريد الإلكتروني، ورقم الهاتف، ورقم الضمان الاجتماعي (Business and professions code sections 22575-22579). وكذلك عناوين بروتوكول الإنترنت، ورغم أن محركات البحث قد ذكرت أنها تتعامل مع تلك العناوين على أنها معلومات غير شخصية، فإن ذلك غير دقيق؛ لأنه ورغم عدم قدرة محركات البحث على تحديد تلك العناوين مباشرة وربطها بمستخدم معين، فإن التحديد يمكن أن يتحقق من جانب طرف ثالث، فمزودو خدمة الإنترنت Internet access providers لديهم بيانات عن عنوان بروتوكول الإنترنت، وتستطيع سلطات إنفاذ القانون والأمن الوطني الوصول إلى هذه البيانات، ويمكن لبعض الأطراف أيضًا الوصول إليها من خلال الدعاوى المدنية. وكذلك ملفات تعريف الارتباط، إذا كانت تحتوي على هوية فريدة للمستخدم unique user ID، فإن هذه الهوية ما هي إلا بيانات شخصية (Article 29 Data Protection Working Party, 2008).

أما المعلومات غير الشخصية، فهي المعلومات التي لا يمكن أن تعود في حد ذاتها إلى فرد بعينه، مثل عنوان آخر موقع URL زاره المستخدم قبل الدخول إلى المحرك، وخصائص المتصفح، ونوع نظام التشغيل في الحاسب الذي يستخدمه المستخدم (Ask, 2008 b)، ونص الاستفسار، وتاريخ الطلب ووقته، والاستجابة للعروض والإعلانات المقدمة من قبل المحرك.

- من الصعب على محرك البحث تحديد هوية باحث معين، استخدمه لإجراء الأبحاث على الإنترنت. إلا أن الحالة تختلف تمامًا عندما يكون المستخدم مُسجلا في المحرك، أو اشترى شيئًا أثناء تواجده على موقعه. حيث يمكن للمحرك في هذه الحالة، ربط المصطلحات التي بحث بها المستخدم عن المعلومات، بأي معلومات محددة للشخصية، قد تطوع وقدمها المستخدم أثناء التسجيل أو الشراء –على افتراض أن هذه المعلومات ليست وهمية- مثل عنوان البريد الإلكتروني، والاسم، وتاريخ الميلاد، والعناوين البريدية، ورقم الهاتف، ومعلومات بطاقة الائتمان (Burke, 2006)، مما يجعل المحرك لديه القدرة على تحديد هوية الباحث.

2/2 المخاوف من جمع محركات البحث لبيانات المستخدمين:

تبين مما سبق التنوع الكبير في المعلومات التي يجمعها المحرك عن المستخدمين، ويثير هذا الكثير من المخاوف التي تتمثل في:

1/2/2 الجهات الحكومية:

تستطيع الحكومات من خلال تقديم مذكرات استدعاء، الحصول على البيانات التي تحتفظ بها محركات البحث عن أبحاث المستخدمين. وقد تقدم الجهات الحكومية الكثير من المبررات لذلك، منها أسباب متعلقة بمحاربة الإرهاب، أو مكافحة مختلف الجرائم التي تقع على الإنترنت. وتُبين التجارب السابقة لتعامل محركات البحث مع مذكرات الاستدعاء من قبل الحكومة، أن تلك المحركات قليلة أو معدومة الحافز لمواجهة استدعاء الحكومة بالرفض، كما أن التزامها يقل أو ينعدم تجاه إخبار المستخدمين بأن سجلاتهم يتم فحصها من قبل الحكومة. ومن الأمثلة على ذلك، مذكرات الاستدعاء التي قدمتها الحكومة الأمريكية في ديسمبر 2005م، إلى كل من Google, Microsoft, Yahoo, AOL لطلب "تواريخ البحث search histories " وعناوين بروتوكول الإنترنت للمستخدمين. وذلك لاحتياجها لبيانات تدعم مشروعها لقانون متعلق بإباحية الأطفال child pornography law ، وقد استجابت تلك المحركات، باستثناء Google الذي رفض ذلك. عندئذ خفضت الحكومة طلبها إلى 50,000 عنوان من عناوين المواقع، و5000 عبارة بحثية أُدخلت من قبل المستخدمين في الفترة من 1يونيه إلى 31يوليو 2005م. وعندما رفض Google الامتثال مرة أخرى، اضطرت الحكومة إلى رفع الأمر إلى المحكمة لإجباره على الامتثال. ولأن المحكمة كانت قلقة من استخدام الحكومة للمعلومات في تحقيقات لا علاقة لها بما ذكرته عن مكافحة إباحية الأطفال، فقد قضت برفض طلبها لآلاف الاستفسارات البحثية التي أجراها المستخدمون عن طريق Google، وطالبت Google بالكشف فقط عن عينة تبلغ 50,000 عنوان من عناوين المواقع التي استخدمها الباحثون، لكنها لم تطالبه بالكشف عن عبارات البحث الخاصة بالمستخدمين (Foley, 2007).

والجدير بالذكر أن كبرى محركات البحث، توجد في الولايات المتحدة الأمريكية. وتُستخدم هذه المحركات على نطاق واسع داخل الولايات المتحدة الأمريكية وخارجها، فعلى سبيل المثال، يُجرى عبر Google وحده حوالي 200مليون بحث يوميًا، أغلبها من خارج الولايات المتحدة (And then there were four). ويعني هذا أن الولايات المتحدة الأمريكية وحكومتها، تستطيع الوصول إلى الملفات المخزن عليها بيانات مستخدمي محركات البحث، مما يسمح لها بمراقبة النشاط البحثي ليس لمواطنيها فقط، ولكن لمواطني الدول الأخرى أيضًا. خاصة أن غالبية محركات البحث قد تستجيب لطلبات الحكومة دون مقاومة، كما رأينا.

2/2/2 إعلان المحركات عن البيانات:

قد تعلن محركات البحث لسبب أو لآخر، عن ملفات البيانات التي تحتفظ بها عن الأبحاث التي أجراها المستخدمون من خلالها. وخير دليل على ذلك، إعلان محرك البحث AOL في أغسطس 2006م ، عن (20) مليون استفسار تم إجراؤها على الويب من قبل (657,000) أمريكي، على مدى 3 شهور هي مارس وأبريل ومايو من العام نفسه، اعتقادًا منه أن إتاحة تلك البيانات سيساعد العلماء، ومن يجرون الإحصاءات لمعرفة المزيد عن كيفية استخدام الأشخاص للإنترنت (McCullagh, 2006). ورغم أن البيانات كانت غير محددة بوضوح من خلال اسم المستخدم، إلا أنها كانت تحتوي في بعض الحالات على معلومات محددة للشخصية، مثل: أسماء وعناوين أفراد، وأسماء مدارس، وأرقام ضمان اجتماعي، وأرقام رخص قيادة، واهتمامات دينية، وحالات طبية محددة ومفصلة، ومعلومات عن التأمين، ومعلومات مصرفية، واستفسارات بحث عن وظائف، ومعلومات عن السفر، وغيرها من المعلومات الشخصية والخاصة للغاية (World Privacy Forum, 2006). وقد تمكنت وسائل الإعلام رغم استخدام المحرك لأرقام بدلا من أسماء الباحثين، وقصر المدة التي بقيت فيها البيانات على موقعه - قبل انتقاد الجماعات المهتمة بالخصوصية له، وإصداره اعتذارًا وإزالته للبيانات- من معرفة أن المستخدم رقم "4417749" هي أرملة تُدعى Thelma Arnold، تبلغ من العمر 62 عامًا، تعيش في Lilburn, Georgia.

وتوضح حالة Thelma Arnold، مدى قدرة محركات البحث على انتهاك الحدود الطبيعية، والاجتماعية، والزمانية والمكانية للمستخدمين. وتتمثل الحدود الطبيعية في العديد من الأشياء، منها: الملابس؛ فالشخص يرتدي الملابس لإخفاء خصائص جسده التي لا يرغب الكشف عنها، وكذلك تعبيرات الوجه والعبارات التي يستخدمها لإخفاء أفكاره ومشاعره الداخلية وحمايتها. بالإضافة إلى الجدران، والأبواب المغلقة، والظلام، وغير ذلك من الوسائل التي يستخدمها لمنع الآخرين من مراقبة سلوكه الخاص. وهناك أيضًا خطوط الهاتف، والبريد الإلكتروني، والرسائل المغلقة، والكلمات السرية لفتح الحاسبات الآلية، وحوائط النار firewalls ، وتشفير البيانات، وغير ذلك من الوسائل التي يستخدمها لحماية معلوماته السرية. ولأن معرفة المصطلحات التي بحثت بها Thelma تكشف لنا عن تأملاتها الخاصة، ورغباتها،

وتأخذنا داخل جدرانها وأبوابها المغلقة، فإن تصرف AOL هو انتهاك لحدودها الطبيعية. ولعل ما عبرت عنه من دهشة وصدمة أثناء المقابلة التي أجرتها مع وسائل الإعلام، لأنها لم تكن تعلم أن هناك من يراقبها، يكشف عن شعور الشخص عند انتهاك الحدود الواقية التي وضعها ليحافظ على خصوصيته.

وتتمثل الحدود الاجتماعية، في حق الشخص في عدم الكشف عن أسراره، أو إساءة التعامل مع سجلاته السرية أو استغلالها. ولأن تواريخ البحث المحفوظة على حاسبات شركات محركات البحث بها معلومات سرية ينبغي عدم إفشائها، فإن AOL قد انتهك الحدود الاجتماعية لـ Thelma؛ حيث كشف عن سجلات بحثها التي تحوي الكثير من أسرارها، دون موافقتها على ذلك.

وتنطوي الحدود الزمانية والمكانية، على حق الشخص في عدم الفصل بين جوانب سيرته الذاتية personal biography، وتقسيمها إلى الماضي والحاضر المستقبل، وإلى أماكن مختلفة. وبالإضافة إلى ذلك، حقه في عدم تسجيل اتصالاته وتفاعلاته العابرة، أو تجزئتها، أو تخزينها، أو إعطائها معنى جديدًا. وقدرة AOL على تخزين "تواريخ البحث"، وتجميعها، ودمجها، والبحث فيها، واسترجاعها، وإعطاء معنى جديد لها، لاشك يخترق الحدود الزمانية والمكانية للشخص، خاصة مع القدرة على تقسيم سيرته الذاتية إلى سمات وفترات مختلفة، وكذلك ينتهك طبيعة اتصالاته وتفاعلاته العابرة. وتتفاقم مشكلة هذه الانتهاكات، إذا لم يكن من الممكن تصحيح المعلومات الخاطئة. والكشف عن بيانات الأبحاث التي أجرتها Thelma خير دليل على ذلك؛ حيث بحثت باستخدام عدة مصطلحات توحي بأنها تعاني من مجموعة كبيرة من الأمراض، إلا أنها أوضحت في المقابلة التي أُجريت معها أن هذا غير صحيح، وأنها تبحث عن المعلومات المتعلقة بالأمراض لمساعدة صديقاتها المريضات (Hillyard and Gauen, 2007).

3/2/2 الرصد التفصيلي لحياة الأفراد:

من المخاوف التي تنشأ عن احتفاظ محرك البحث ببيانات المستخدمين، قدرته على ربط تلك البيانات معًا، مما يمكنه من الرصد التفصيلي لحياة مستخدميه. وعلى سبيل المثال، إذا سجل المستخدم لدى إحدى إعلانات المحرك، فإن المحرك سيعرف تفصيلات حسابه المصرفي وعنوان منزله. وإذا كان لدى الشخص مدونة في خدمة المدونات التي يوفرها المحرك، فإن المحرك سيعرف ذلك أيضًا. كما يمكن للمحرك معرفة الخرائط التي بحث فيها المستخدم، إذا كان المحرك يقدم خدمة البحث في الخرائط. بالإضافة إلى أنه يعرف عنوان البريد الإلكتروني للمستخدم، ويمكنه الوصول لمحتوى الرسائل في هذا البريد، إذا كان لدى المستخدم حساب بريد إلكتروني على هذا المحرك. ولا يتوقف الأمر عند ذلك، بل لدى المحرك القدرة على رصد سمات تفصيلية لاهتمامات المستخدمين من خلال أبحاثهم، فيمكن أن تعكس استفسارات البحث عادات المستخدم القرائية على الإنترنت، وتاريخه الطبي، وشؤونه المالية، وخططه، ورغباته، ومصالحه،

وانتمائه السياسي، ومعتقداته الدينية،..... . ولنرى المثال الآتي، وهو مأخوذ من البيانات التي أعلنها محـــرك البحـــث AOL في أغسطس 2006م، للمستخدم رقم 14162375، القاطن في ولاية فلوريدا [يمكن معرفة مكان إجراء البحـــث من خلال عنوان بروتوكول الإنترنت] (Brown, 2006):

March
marriage counseling 2006-03-19 17:50:31
spy on the wife 2006-03-19 17:52:47
spy recorders 2006-03-19 18:02:34
signs of cheating 2006-03-19 18:05:52
tracking cell phone numbers 2006-03-21 11:00:13
divorce 2006-03-23 14:10:27
saving a marriage 2006-03-26 23:50:11
stop your divorce 2006-03-27 23:49:06
alchool withdrawl 2006-03-28 10:43:51
cheating therapy 2006-03-30 16:49:56
spy from a distance 2006-03-31 21:11:29
listen through walls 2006-03-31 21:16:25
car conversation spy 2006-03-31 21:20:24

April
spy on wife 2006-03-31 21:21:29
i want my wyfe back 2006-04-02 23:14:28
i want revenge to my wife 2006-04-02 23:27:54
divorce and kids 2006-04-03 12:19:46
llllfkkgjnnvjjfokrb 2006-04-03 18:20:11
vvvvbmkmjk 2006-04-03 18:20:36
vvglhkitopppfoppr 2006-04-03 18:22:04
my wife wants to leave me 2006-04-07 16:35:03
how do i get my wife love me again 2006-04-08 17:10:55
my wife doesnt love animore 2006-04-08 19:30:58
making my wife suffer as i do 2006-04-09 13:19:54
husband revenge 2006-04-09 15:23:37
how to harm my wifes lover 2006-04-10 13:11:28
catch your wife aving an affair 2006-04-10 14:44:32
my cheating wife 2006-04-16 16:48:06
i want to kill myself 2006-04-16 19:55:51
kill my wifes mistress 2006-04-16 20:26:49
cheating wives 2006-04-18 16:45:12
recording home surveillance 2006-04-18 16:54:53

May
private eye 2006-05-30 21:12:07
video surveillance 2006-05-30 21:21:24

يتبين لنا من المثال السابق أن المحرك قادر على رصد الحالة النفسية وما يفكر فيه الشخص، كل ذلك مسجلا ليس فقط باليوم والساعة والدقيقة، بل وبالثانية أيضًا. حيث استطعنا معرفة أن هناك خلافات بين المستخدم وبين زوجته، التي يشك في سلوكها، مما جعله يحاول مراقبتها باستخدام وسائل المراقبة السمعية والبصرية. ورغبته في استرجاعها والانتقام منها، وتفكيره في طلاقها، وتأثير الطلاق على الأبناء، كما استطعنا أن نستشعر أن الساعة السادسة والربع من اليوم 2006/4/3م ، كانت أقسى لحظات الإحباط والاضطراب النفسي التي مر بها هذا الشخص، مما جعله يدخل حروفًا هجائية لا معنى لها في مربع البحث بالمحرك. ولولا أن المدة التي كشف عنها AOL انتهت عند هذا الحد، لكان من المؤكد أننا سنعرف كيف انتهت تلك القصة، التي تقع أحداثها الحقيقية في ولاية فلوريدا؟؟!!

4/2/2 سرقة البيانات أو مهاجمتها:

قد يتم سرقة البيانات المخزنة عن المستخدمين أو مهاجمتها من قبل قراصنة الإنترنت hackers، أو حتى من المتصفحين العاديين، إذا لم تكن قواعد البيانات المخزنة فيها آمنة بالشكل اللازم (Ham). وقد أبدت بعض محركات البحث، تخوفًا من عدم وجود نظام آمن 100 ٪ ، وبالتالي أخلت مسؤوليتها عن ضمان أمن المعلومات التي تجمعها عن المستخدمين على الإنترنت (Ask, 2008 b)!!!

5/2/2 بيع البيانات:

يمكن لمحركات البحث بيع البيانات التي تجمعها عن المستخدمين وعن أبحاثهم، إلى الشركات التجارية (Erickson and Bankston, 2006).

6/2/2 اندماج الشركات:

قد يؤدي اندماج الشركات المالكة لمحركات البحث، مع شركات أخرى إلى دمج البيانات التي جُمعت عن الأفراد في كل من الشركتين في قواعد بيانات واحدة، ويكمن الخطر في إمكانية ربط تلك البيانات معًا، ويعطي هذا للشركات فرصة الوصول إلى كم لا نهائي من المعلومات عن الأفراد (Edwards, 2007).

3/2 أساليب جمع محركات البحث لبيانات المستخدمين:

من أهم الأساليب التي تستخدمها محركات البحث (عينة الدراسة) لجمع بيانات المستخدمين:

1/3/2 المستخدم نفسه:

حتى يستطيع المستخدم الاستفادة من بعض خدمات محرك البحث، فعليه التسجيل لدى المحرك. ويستدعي هذا تقديم الكثير من المعلومات الشخصية للمحرك.

2/3/2 عنوان بروتوكول الإنترنت: IP address

عنوان بروتوكول الإنترنت هو رقم فريد يُعطى لكل كمبيوتر من قبل مزود خدمة الإنترنت، وهذه الأرقام مقسمة وفقًا للدول، لذا عادة ما يُستخدم عنوان بروتوكول الإنترنت لتحديد الدولة التي اتصل منها الحاسب بالإنترنت (Google, 2008 a). بالإضافة إلى معرفة بيانات أخرى، منها: اسم المضيف، ووكيل المستخدم، ونظام التشغيل، ونوع المتصفح، ودقة الشاشة Resolution، وجودة الألوان Color Depth، واللغة المستخدمة، وما إذا كان وكيلا Proxy أم لا ..... (http://myipinfo.net/)،

ويمكن لمحرك البحث ربط مختلف الاستفسارات الخاصة بعنوان بروتوكول إنترنت واحد. ومن ثم يستطيع تعقب جميع الأبحاث على الإنترنت، التي مصدرها عنوان بروتوكول إنترنت واحد وربطها معًا (Article 29 Data Protection Working Party, 2008).

3/3/2 ملفات تعريف الارتباط: Cookies

ملفات تعريف الارتباط هي ملفات برمجية صغيرة تحتوي على سلسلة من البيانات، يتم تثبيتها على الحاسبات دون معرفة الشخص (Brandt, 2002)، من قِبل المواقع على الإنترنت، لفترة محددة مسبقًا. ولعل من أهم الفوائد التي توفرها ملفات تعريف الارتباط، التعرف إلى خيارات المستخدم عند إجراء الأبحاث مثل اللغة أو اللغات التي يرغب في البحث فيها، وعدد المواقع التي يرغب في عرضها في صفحة نتائج البحث الواحدة، ودعم الإجراءات الأمنية، على سبيل المثال طلب إعادة الدخول re-logging لمنتج أو خدمة ما لدى المحرك بعد مضي وقت من الزمن (Yahoo, 2008 d)....

ويتم استعادة ملفات تعريف الارتباط عادة من جانب موقع الإنترنت الذي ثبتها فقط؛ أي أن المواقع لا يمكنها الاطلاع على الملفات التي ثبتتها المواقع الأخرى. وهناك نوعان من ملفات تعريف الارتباط: ملفات تعريف الارتباط الدائمة، وملفات تعريف الارتباط غير الدائمة. تقوم ملفات تعريف الارتباط غير الدائمة بتخزين بيانات مؤقتة على متصفح المستخدم، وتُدمر عند خروجه من المتصفح. أما ملفات تعريف الارتباط الدائمة، فهي البيانات التي ثبتها الخادم جنبًا إلى جنب مع تاريخ انتهاء صلاحية تلك الملفات، وخزنها على المتصفح الخاص بالمستخدم حتى تاريخ انتهاء صلاحيتها (Duberman and Beaudet, 2000).

ويسمح استخدام ملفات تعريف الارتباط الدائمة لمحرك البحث بربط مختلف الاستفسارات الخاصة بملفات تعريف ارتباط واحدة. ومن ثم يمكن تعقب جميع الأبحاث على الإنترنت، الصادرة عن حاسب آلي بعينه، حتى مع استخدام عنوان بروتوكول متغير وربطهما معًا(Article 29 Data Protection Working Party, 2008) .

4/3/2 عدادات الشبكة: web beacons

تستخدم محركات البحث، عدادات الشبكة web beacons ، وعلامات بكسل pixel tags, وهي برمجيات تسمح بتتبع استخدام المستخدم للمحرك، بغرض إحصاء المستخدمين الذين زاروا صفحة ما، ومحاسبة المعلنين، والوصول إلى ملفات تعريف ارتباط محددة (Yahoo, 2008 c) .

5/3/2 شريط الأدوات ومُسرِّع الويب: Toolbar and Web Accelerator

عند تثبيت شريط الأدوات ومُسرِّع الويب، اللذين تقدمهما بعض محركات البحث، كخدمة لمستخدميها، فإن هذه البرمجيات يمكن أن ترسل معلومات إضافية عن المستخدم للمحرك، مثل: عناوين المواقع URL التي زارها، وأية معلومات شخصية مُضمنة في هذه العناوين، ونص الاستفسارات الذي بحث عنها (Google, 2008 a).

6/3/2 سجلات مركز الخدمة: Server logs

تسجل مراكز الخدمة في محركات البحث آليًا الطلبات التي ينشئها المستخدمون عند زيارتهم لتلك المحركات. وتتضمن "سجلات مركز الخدمة" عادةً طلب الويب الخاص بالمستخدم، وعنوان بروتوكول الإنترنت الخاص به، ونوع المتصفح، ونظام التشغيل، وتاريخ الطلب ووقته، وواحد أو أكثر من ملفات تعريف الارتباط Cookies. وفيما يلي مثال لقيد سجل في محرك البحث Google، حيث يتم البحث عن "سيارات" (Google, 2008 a):

123.45.67.89 - 25/Mar/2003 10:15:32 - http://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

وفيما يلي تحليل لمكونات هذا المثال:

- الرقم 123.45.67.89 : هو عنوان بروتوكول الإنترنت المُخصَّص للمستخدم عن طريق مزود خدمة الإنترنت (ISP).
- 25/Mar/2003 10:15:32 : هما تاريخ الاستفسار ووقته.
- http://www.google.com/search?q=cars : هو عنوان الموقع URL المطلوب مشتملاً على استفسار البحث.
- Firefox 1.0.7; Windows NT 5.1 : هما إصدارا المتصفح ونظام التشغيل المستخدمان.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

- 740674ce2123e969 : هو التعريف الفريد لملف تعريف الارتباط المُخصَّص لهذا الحاسب في أول مـــرة زار فيها موقع Google.

7/3/2 تاريخ البحث: Search History

هناك نوعان من تاريخ البحث، النوع الأول تحتفظ به جميع المحركات، بعيدًا عن يد المستخدم. والنوع الثاني، تقدمـــه بعض المحركات للمستخدمين وتسمح لهم بالوصول إليه. والنوع الأول يتشابه إلى حد كبير مع "سجلات مركز الخدمة "، وأحيانًا يتطابق معه، فتُطلق عليه المحركات "تاريخ البحث" بدلا من "سجلات مركز الخدمة ". وهناك من يرى أن خدمة "تاريخ البحث" رغم الفوائد التي توفرها للباحثين، يكمن وراء تقديمها دوافع اقتصادية؛ فـــيمكن للقـــائمين علـــى أمـــر المحركات من خلال قواعد البيانات المتعلقة بتلك الخدمة، تقديم بيانات عن سمات الباحثين إلى المعلنين. والأخطر مـــن ذلك هو احتمال وجود دوافع سياسية لتقديمها، فهي لا تسمح فقط بمعرفة ما يفعله الإنسان، ولكن أيضًا ما يُفكـــر فيـــه. والخطورة في ذلك، أن مثل هذا الرصد يمكن استخدامه في المراقبة وقمع المعارضة السياســـية فـــي نهايـــة المطـــاف (Hinman, 2005).

أما النوع الثاني فتقدمه بعض محركات البحث، ومن أمثلتها Google ، AOL Search. حيـــث يقـــدم Google خدمـــة "Web History"، التي تسمح للمستخدم بعرض النص الكامل للصفحات التي زارها من قبل والبحث خلالها، ويشـــتمل ذلك على الأبحاث، وصفحات الويب، والصور، والفيديو، والأخبار. وكذلك تمكنه من إدارة نشاطه على الويب من خلال حذف الوحدات التي لا يريدها في web history في أي وقت. وتجعله يحصل على نتائج بحث أكثر صلة بـــه، وذلـــك اعتمادًا على ما يبحث عنه المستخدم في Google والمواقع التي زارها. وتسمح له أيضًا بمعرفة اتجاهات اهتماماته في أنشطته على الويب، مثل ما هي المواقع التي يزورها باستمرار؟ وما عدد الأبحاث التي أجراها خـــلال فتـــرة زمنيـــة محددة؟ (Google, 2008 c) . ومن الواضح أن هذا الأسلوب يسهل عملية جمع كل الأنشطة التي قام بها المستخدم مـــن خلال Google على الويب في مكان واحد. كما أن الاستفادة من هذه الخدمة يستدعي "التســـجيل"، ممـــا يعنـــي تقـــديم المستخدم لمزيد من المعلومات عن نفسه للمحرك.

كما يقدم محرك البحث AOL Search خدمة تسمى "Search History" وهي تسمح للمستخدم بتسجيل ما أجراه علـــى المحرك من أبحاث لمدة (30) يومًا، وتمكنه من حذف هذه البيانات في أي وقت يشاء، وتسمح له أيضًا بإيقاف عمل هذه الخدمة تمامًا (AOL, 2008 b). وتختلف هذه الخدمة عن الخدمة التي يقدمها Google حيث لا تستدعي التسجيل.

8/3/2 المواقع التابعة: Affiliated sites

قد تقدم محركات البحث بعضًا من خدماتها عبر مواقع ويب أخرى. وقد يتم إرسال المعلومات الشخصية التي يقدمها المستخدم للمواقع إلى تلك المحرك لكي يتم توفير الخدمة التي يريدها المستخدم (Google, 2008 b).

نستنتج من العرض السابق أن محركات البحث، تلجأ إلى أساليب عدة لجمع البيانات عن المستخدمين. وبصفة عامة يمكن تقسيم المعلومات التي تُجمع عن المستفيدين في محركات البحث وفقًا لأساليب جمعها، إلى فئتين: تشتمل الفئة الأولي على المعلومات التي يقدمها الشخص طواعية عند الرغبة في التسجيل لدى المحرك، للاستفادة من بعض خدماته. وتشتمل الفئة الثانية على معلومات يتم جمعها دون علم المستخدم من خلال التقنية التي تستخدمها تلك المحركات.

4/2 أسباب جمع محركات البحث لبيانات المستخدمين:

تشتمل الأسباب التي تدعو محركات البحث (عينة الدراسة) لجمع بيانات المستخدمين، على:

- عدم وجود القوانين الكافية لحماية خصوصية أبحاث المستخدم، ومعاقبة المحركات إذا انتهكت تلك الخصوصية (Raysman and Brown, 2007).
- تشغيل وتطوير مواقع الويب، والخدمات والعروض المتاحة عن طريق المحرك.
- إضفاء الطابع الشخصي على المحتوى والإعلانات المقدمة، أو ما يُطلق عليه "الإعلانات الموجهة أو المخصصة".

ويمكن القول بأن هذا السبب، من أهم الأسباب وراء جمع المحركات للمعلومات عن المستخدمين؛ لأن الإعلانات هي مصدر التمويل الأساسي للمحركات. وعادة ما تتم محاسبة المُعلن فقط عن الإعلانات التي يضغط click عليها المستخدم (Aggarwal, 2005)، لذا يبذل القائمون على أمر المحرك قصارى جهدهم لضمان ضغط المستخدم على الإعلانات. فنجد أن المحرك يراقب نوع المحتوى الذي وصل إليه المستخدم، والاستفسارات البحثية التي طلبها، ليتم عرض الإعلانات ذات الصلة بها، فعلى سبيل المثال الأشخاص الذين يبحثون عن نتائج الجولف يتم عرض إعلانات لهم تتعلق بمنتجات وخدمات لها صلة بتلك اللعبة. كما يجمع المحرك البيانات التي يستطيع عن طريقها تحديد مكان وجود المستخدم، من خلال الرقم البريدي الذي يسجله، أو من خلال عنوان بروتوكول الإنترنت الخاص به، وذلك لعرض إعلانات تتناسب مع ذلك المكان. وتستخدم أيضًا المعلومات التي سجلها المستخدم مع خدمات المحرك مثل النوع، والعمر، والوظيفة، لعرض الإعلانات المناسبة لتلك السمات (Yahoo, 2008 a).

- انجاز طلبات المستخدمين للحصول على المنتجات، والبرامج، والخدمات.
- التواصل مع المستخدمين، والرد على استفساراتهم.
- المساعدة في تقديم منتجات أو برامج أو خدمات جديدة، قد تكون موضع اهتمام المستخدمين (AOL, 2008 a).
- إجراء الأبحاث والتحليل بهدف الحفاظ على خدمات المحرك وحمايتها وتحسينها.

- مكافحة انتهاكات شروط استخدام المحرك، أو معالجة المشاكل الأمنية أو الفنية التي يتعرض لها، أو الحماية من أي ضرر وشيك بحقوقه أو ممتلكاته أو سلامة موظفيه.
- اكتشاف مشاكل الاحتيال، أو الحماية من أي ضرر وشيك بحقوق أو ممتلكات أو سلامة المستخدمين أو عامة الناس (Google, 2008 b).
- تقديم تقارير مجمعة لا تكشف عن هوية المستخدمين لعملاء داخليين أو خارجيين.
- إعادة الهيكلة، ويتضمن ذلك: حدوث عمليات دمج للمحرك، أو امتلاك، أو أي شكل من أشكال البيع لبعض ممتلكاته أو كلها (Yahoo, 2008 e).
- المطالب القانونية، ويتضمن ذلك: تنفيذ أي قانون معمول به، أو لائحة، أو إجراء قانوني، أو مطلب حكومي واجب التنفيذ، أو ممارسة المحرك لحقوقه القانونية أو الدفاع ضد الإدعاءات القانونية الموجهة إليه (Ask, 2008 b).

نستنتج مما سبق، تنوع الأسباب التي تدعو محركات البحث لجمع البيانات من المستخدمين أو عنهم، فهناك أسباب تتعلق بالمحركات نفسها ورغبتها في تحسين خدماتها الحالية وتقديم خدمات جديدة، وتخصيص المحتوى والإعلانات للحصول على الأموال، وحماية ممتلكاتها وموظفيها. ومنها ما يتعلق بالمستخدم نفسه، مثل الاتصال به، والوفاء بطلباته، وتخصيص المحتوى المقدم له. وترى الباحثة أن الاحتفاظ بالبيانات عن المستخدمين لصالح المحرك بالدرجة الأولى، ولصالح المستخدم بالدرجة الثانية.

5/2 فترات احتفاظ المحركات ببيانات البحث:

بينت الدراسات أن محركات البحث (عينة الدراسة) كانت في البداية تحتفظ بالمعلومات التي جمعتها من المستخدمين أو عنهم [بما في ذلك البيانات المتعلقة بالأبحاث] طالما أن لها فائدة، أي أن المحركات كان يمكنها الاحتفاظ بها إلى الأبد. كما أن ملفات تعريف الارتباط الخاصة بها كان من المكن أن تبقى لسنوات طويلة قبل حذفها من على حاسب المستخدم، ومنها على سبيل المثال ملفات تعريف الارتباط الخاصة بـ Google التي صرح بأنها ستبقى حتى عام 2038م (McCullagh and Mills, 2007).

وقد وجهت الجهات المراقبة للخصوصية privacy watchdogs، والاتحاد الأوروبي، انتقادات شديدة لمحركات البحث لاحتفاظهم ببيانات المستخدمين لهذه الفترات الطويلة. وفي محاولة لتهدئة تلك الانتقادات، أعلنت المحركات أنها ستضع حدودًا أقصر لفترات احتفاظها ببيانات المستخدمين (Google Reduces Data Retention Period, 2007). ويوضح الجدول الآتي رقم (2) فترات احتفاظ المحركات (عينة الدراسة) ببيانات البحث.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

الجدول رقم (2)

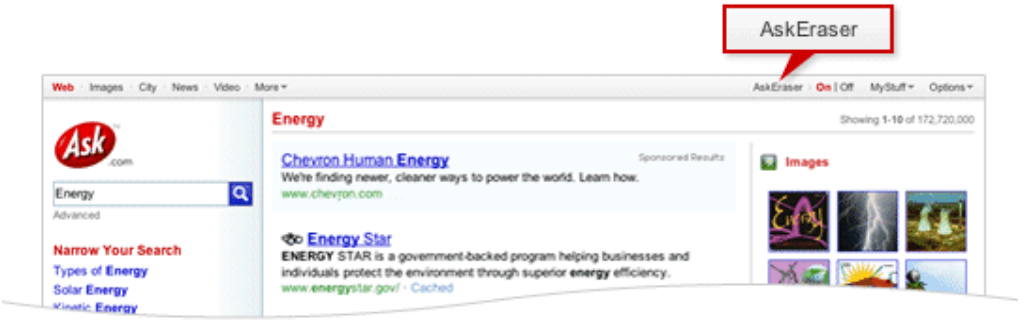
فترات احتفاظ المحركات ببيانات البحث

البيان / المحركات	فترات الاحتفاظ ببيانات البحث		
	عنوان بروتوكول الإنترنت	رقم هوية ملف تعريف الارتباط	الاستفسار
AOL	13 شهر	13 شهر	13 شهر
Ask مستخدمو AskEraser	بضع ساعات	بضع ساعات	بضع ساعات
المستخدمون الآخرون	18 شهر	18 شهر	غير محدد
Google	18 شهر	18 شهر	غير محدد
Microsoft	18 شهر	18 شهر	غير محدد
Yahoo	13 شهر	13 شهر	غير محدد. بعض الاستفسارات سيتم حذفها تلقائيًا بواسطة مرشح المعلومات الشخصية بعد 13 شهر

(المصدر: Center for Democracy Technology, 2007.)

بين الجدول السابق رقم (2) أن فترات الاحتفاظ بعناوين بروتوكول الإنترنت، وأرقام هوية ملفات تعريف الارتباط، بلغت 18 شهرًا في كل من Ask (المستخدمون العاديون)، و Google، و Microsoft، إلا أنهم لم يحددوا فترات الاحتفاظ بالاستفسارات. وبلغت فترة الاحتفاظ بعناوين بروتوكول الإنترنت، وأرقام هوية ملفات تعريف الارتباط، والاستفسارات 13 شهرًا في AOL. أما محرك البحث Yahoo فقد تماثل وضعه مع AOL، باستثناء مدة الاحتفاظ بالاستفسارات، حيث لم يحددها، وإن كان يحذف بعض الاستفسارات تلقائيًا بواسطة مرشح المعلومات الشخصية بعد 13 شهرًا.

أما محرك البحث Ask -وبالإضافة إلى ما سبق ذكره- فإنه يقدم خدمة تُعرف باسم "AskEraser" [انظر الشكل رقم (1)]، تُمكن المستخدم من مسح النشاط المتعلق بأبحاثه من خوادم Ask.com خلال ساعات، باستثناء بعض الحالات التي يحتفظ فيها المحرك بالبيانات لفترة أطول، ومنها حاجة المحرك إلى تشغيل برامج آلية لاكتشاف المستخدمين الذين يسيؤون استخدامه ومنعهم من ذلك، أو وجود مشكلات فنية، أو وجود طلب قانوني (Ask, 2008 a) .



الشكل رقم (1)

مكان وجود AskEraser على موقع محرك البحث Ask

ورغم تخفيض محركات البحث لفترات احتفاظها بعناوين بروتوكول الإنترنت، وأرقام هوية ملفات تعريف الارتباط، والاستفسارات، فإنها ما زالت –باستثناء Ask عند تفعيل AskEraser- غير متطابقة مع المعيار الذي وضعته الهيئة الاستشارية الأوروبية The Article 29 Working Party ، والذي بينت فيه عدم وجود سبب يدعو محركات البحث للاحتفاظ بالمعلومات البحثية عن المستخدمين لمدة تزيد عن ستة أشهر. كما أوصت، أن على محركات البحث تقديم "مبررات كافية"، لتوضيح الأسباب التي تدعوها للاحتفاظ بالبيانات بعد هذه المدة. وفي تبرير منها، ذكرت محركات البحث أنها تحتفظ بسجلات البحث لأن Data Retention Directive يطلب من شركات الاتصالات الاحتفاظ بسجلات الاتصالات لمدة تتراوح من ستة أشهر إلى 24 شهرًا، وذلك [تحسبًا] لحاجة وكالات تنفيذ القانون لها. ولكن The Article 29 Working Party قالت إن هذا التوجيه ينطبق على شركات الاتصالات، لا على مزودي محتوى الإنترنت (EU Panel: Delete Search Info Sooner, 2008).

وفي الواقع هناك قلق دائر بين أوساط المهتمين بالخصوصية، حيث يرون أن تحديد فترة الاحتفاظ بملفات تعريف الارتباط، ما هي إلا خدعة كبيرة من محركات البحث. لأنها تستطيع تثبيت ملفات تعريف ارتباط جديدة بمجرد انتهاء

فترة حياة القديمة ولنفس المدة المحددة، وهكذا تستمر الدائرة المفرغة إلى ما لا نهاية (Dan, 2007). وما يزيد القلق هو الخوف من قدرة محركات البحث على ربط أرقام هوية ملفات تعريف الارتباط الجديدة بالقديمة، مما يعني القدرة على ربط المعلومات البحثية والشخصية للمستخدم بشكل متواصل، رغم تحديد العمر الافتراضي لملفات تعريف الارتباط المثبتة على حاسبه من قبل المحرك.

6/2 حذف المحركات لبيانات البحث:

يبين الجدول الآتي رقم (3) كيفية حذف المحركات (عينة الدراسة) لبيانات البحث والتخلص منها.

الجدول رقم (3)

حذف المحركات لبيانات البحث

البيان / المحركات	حذف بيانات البحث		
	عنوان بروتوكول الإنترنت	رقم هوية ملف تعريف الارتباط	الاستفسار
AOL	حذف كامل للعنوان	حذف كامل لرقم الهوية	الاحتفاظ فقط بإحصاءات مجمعة عن تكرار الاستفسار
Ask مستخدمو AskEraser	حذف كامل للعنوان	حذف كامل لرقم الهوية	حذف كامل للاستفسار
المستخدمون الآخرون	حذف كامل للعنوان أو آخر ثمانية أرقام	حذف كامل لرقم الهوية	لا يُحذف
Google	حذف آخر ثمانية أرقام من العنوان	حذف كلي أو جزئي لرقم الهوية	لا يُحذف
Microsoft	حذف كامل للعنوان	حذف كامل لرقم الهوية	لا يُحذف
Yahoo	حذف آخر ثمانية أرقام من العنوان	حذف جزء من رقم الهوية	استخدام مرشح المعلومات الشخصية لحذف الأسماء، والعناوين، وأرقام الهواتف...

(المصدر: Center for Democracy Technology, 2007)

نلاحظ من الجدول السابق رقم (3)، ما يأتي:

- يحتفظ محرك البحث AOL بالاستفسارات في شكل مُجمع، ويحذف جميع عناوين بروتوكول الإنترنت، وملفات تعريف الارتباط. ويقضي هذا على إمكانية ربط عمليات بحث المستخدمين.
- يعطي محرك البحث Ask المستخدمين خيار حذف كل من عناوين بروتوكول الإنترنت، وملفات تعريف الارتباط، ومعلومات استفسار البحث. وذلك من خلال استخدام AskEraser.
- يحذف Google جزئيًا معلومات عنوان بروتوكول الإنترنت، وملفات تعريف الارتباط المحددة للهوية جزئيًا (أو ربما بالكامل). ويقطع حذف هذه المعلومات شوطًا بعيدًا نحو الحد من إمكانية ربط استفسارات البحث إلى مستخدمين معينين.
- أخذ Microsoft نهجًا مختلفًا، وهو التخلص من جميع المُحددات الفريدة. وهذا يجعل من الصعب للغاية، إذا لم يكن من المستحيل، ربط استفسارات البحث بمستخدمين محددين.
- يحتفظ Yahoo جزئيًا بعناوين بروتوكول الإنترنت، وملفات تعريف الارتباط المحددة للهوية، بالإضافة إلى استخدام مرشح المعلومات الشخصية personal information filter لإزالة الأسماء، والعناوين، وأرقام الهاتف، وأرقام الضمان الاجتماعي، وغير ذلك من المعلومات الشخصية، والتي قد يكون المستخدم كتبها في مصطلحات بحثه. ودمج هذا الحذف مع تطبيق مرشحات المعلومات الشخصية، يقلل من احتمال ربط سجلات البحث الخاصة بمستخدمين معينين.

نستنتج مما سبق أن محرك البحث Ask هو أفضل محركات البحث (عينة الدراسة)، فيما يتعلق بقضيتي فترات الاحتفاظ ببيانات البحث وكيفية حذفها، شريطة استخدام خدمة "AskEraser".

وبصفة عامة يمكن القول، بأن وجود مثل هذا النهج في أكبر محركات البحث، هو علامة إيجابية دالة على أنها تعمل على توفير طرق لتحسين حماية الخصوصية (Center for Democracy Technology, 2007). وربما يخفف ذلك من القلق الذي تم الإشارة إليه في السابق، والمتعلق بالخوف من قدرة محركات البحث على الاحتفاظ ببيانات البحث التي يقوم بها المستخدمون رغم تحديده لفترات احتفاظه بها.

7/2 مشاركة بيانات البحث مع جهات أخرى، وموافقة المستخدم على ذلك:

قد تتشارك محركات البحث في المعلومات التي تجمعها من المستخدمين أو عنهم، مع جهات أخرى، بما في ذلك بيانات أبحاثهم، وخاصة إذا كانت المحركات تربط بين المعلومات الشخصية للمستخدمين مع البيانات المتعلقة بأبحاثهم. وقد تبين للباحثة في دراسة سابقة لها أن الأسباب التي تدعو محركات البحث (عينة الدراسة) للكشف عن معلومات

المستخدمين لديهم أو مشاركة الغير فيها، تتمثل في: تقديم الإعلانات، أو معالجة رسائل البريد وتسليمها، أو توفير دعم العملاء، أو استضافة مواقع ويب، أو معالجة المعاملات المالية والتجارية، أو تحليل إحصائي لخدمات المحرك، أو معالجة المعلومات الشخصية نيابة عن المحرك. وكذلك تنفيذ أي قانون معمول به، أو لائحة، أو إجراء قانوني، أو مطلب حكومي واجب التنفيذ، أو ممارسة المحرك لحقوقه القانونية، أو الدفاع ضد الادعاءات القانونية الموجهة إليه. أو حدوث انتهاكات لشروط استخدام المحرك، أو حدوث مشاكل أمنية أو فنية له، أو الحماية من أي ضرر وشيك بحقوقه أو ممتلكاته أو سلامة موظفيه. وكذلك عند الحاجة إلى اكتشاف مشاكل الاحتيال، أو الحماية من أي ضرر وشيك بحقوق أو ممتلكات أو سلامة المستخدمين أو عامة الناس. بالإضافة إلى الأسباب المتعلقة بحدوث عمليات دمج للمحرك، أو امتلاك، أو أي شكل من أشكال البيع لبعض أو لكل ممتلكاته. وقد لا تكشف المحركات ليس فقط عن المعلومات الشخصية، أو المجمعة للمستخدمين، بل أيضًا عن محتوى اتصالاتهم على الإنترنت (أحمد، قيد النشر).

وفيما يتعلق بموافقة المستخدم على مشاركة المحرك لبيانات بحثه مع أطراف أخرى، فقد تبين أن سياسات الخصوصية في بعض محركات البحث، تنص على أن استخدام الشخص للخدمات التي يقدمها المحرك، أو تسجيله لدى المحرك، تعني موافقته على نقل المعلومات الخاصة به لمرافق المحرك والأطراف الأخرى (Ask, 2008 b). ويعني هذا أيضًا أن هناك موافقة قد أُخذت من المستخدم تسمح للمحرك بالتصرف كيفما شاء في المعلومات التي جمعها عنه دون الرجوع إليه، ويزداد الأمر سوءً إذا علمنا أن غالبية المستخدمين لا يقرؤون سياسات الخصوصية الموجودة في المحركات، مما يعني أن المستخدم قد وافق على السماح للمحرك بمشاركة بياناته والكشف عنها، دون أن يدري حتى إنه وافق على ذلك!!! وترى الباحثة أن هذا الوضع ينبغي مراجعته، وأن يتم إعلام المستخدم صراحة عند إجراء بحثه، أن هناك معلومات تُجمع عنه، وتؤخذ موافقة صريحة منه تسمح للمحرك بمشاركة هذه المعلومات مع أطراف أخرى، وإذا لم يوافق المستخدم على هذا، فيجب على المحرك ألا يكشف عن هذه المعلومات للأطراف الأخرى.

8/2 حذف المستخدمين لبيانات أبحاثهم:

تتيح محركات البحث للمستخدمين تعديل معلوماتهم في حساباتهم الشخصيةuser Account ، إما بالتصحيح أو الحذف. إلا أن الوضع يختلف مع بيانات البحث؛ حيث أمكن للباحثة رصد ثلاثة أساليب تتعامل من خلالها المحركات مع تلك القضية:

الأسلوب الأول: لا توفر فيه المحركات الفرصة أمام المستخدمين للوصول إلى البيانات المتعلقة بأبحاثهم أو حذفها، وقد أُستخدم هذا الأسلوب في كل من Yahoo ، و Live Search .

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

الأسلوب الثاني: تتيح فيه المحركات التي تقدم خدمة "تاريخ البحث" للمستخدم، الوصول إلى البيانات المخزنة عن طريق هذه الخدمة وحذفها. وقد أُستخدم هذا الأسلوب في كل من Google، وAOL Search. ومن الواضح أن هذا الأسلوب يسمح للمستخدمين بحذف البيانات من "تاريخ البحث" فقط، إلا أنه لا يحذفها من خوادم المحركات.
الأسلوب الثالث: تسمح فيه المحركات للمستخدمين بحذف البيانات المتعلقة بأبحاثهم من الخوادم، وقد أُستخدم هذا الأسلوب في Ask فقط، من خلال خدمة AskEraser، التي تسمح للمستخدم بمسح نشاطه المتعلق بالأبحاث من خوادم ذلك المحرك، إلا في بعض الحالات الاستثنائية التي سبق ذكرها.

والجدير بالذكر أن المحركات قد لا تقوم بحذف البيانات، حتى بعد طلب المستخدم ذلك، لأسباب عدة، منها وجود طلب قانوني للتحفظ على تلك البيانات، أو غير ذلك. بالإضافة إلى أن حذف البيانات من خوادم المحركات، لا يعني حذفها نهائيًا، حيث يمكن للمحركات الاحتفاظ بهذه البيانات في النسخ الاحتياطية لفترة من الزمن (Yahoo, 2008 b)!!!

3. طرق مقترحة لحماية خصوصية البحث على الإنترنت:

لا يوجد في الوقت الحاضر حل سهل يضمن خصوصية كاملة لأنشطة بحث المستخدم على الإنترنت، نظرًا لقدرة محركات البحث على الاحتفاظ بالمعلومات التي يرسلها المستخدم خلال الإنترنت، وتخزينها بواسطة مجموعة متنوعة مترابطة من النظم، ولكن إتباع الاقتراحات الآتية، يوفر حماية لخصوصية المستخدمين إلى حد كبير. وهناك ثلاث فئات أساسية يمكن تقسيم الاقتراحات على أساسها، وهي: الدول، ومحركات البحث، والمستخدم نفسه:

1/3 دور الدول:

إن الدور الأساسي المنوط بالدول، هو وضع القوانين والتشريعات، لتقنين خصوصية البحث على الإنترنت. وفي الواقع، توجد عدة قوانين ترتبط بحماية خصوصية الأفراد أثناء استخدامهم للإنترنت وخدماتها، ومن أهم هذه القوانين: قانون خصوصية الاتصالات الإلكترونية "Electronic Communications Privacy Act "ECPA، الذي يحمي الأفراد من التدخلات الحكومية والخاصة أثناء اتصالاتهم الإلكترونية، ولا يسمح بالكشف عنها دون إذن من المحكمة (Burke, 2006). وتوجد وجهتا نظر مختلفتان حول هذا القانون، يرى أصحاب وجهة النظر الأولى، أنه وفقًا لهذا القانون، فإن "الاتصال الإلكتروني" يعني "أي نقل للعلامات، والإشارات، والكتابة، والصور، والأصوات، والبيانات"، ويشير "المحتوى" إلى "أي معلومات تتعلق بفحوى، أو معنى هذا الاتصال"، إذن تقع بيانات البحث الخاصة بمستخدم الإنترنت في إطار حماية ECPA؛ وذلك لأن المستخدم عندما يحيل مصطلح البحث من خلال المحرك مثل Google، فإنه يُحيل "الكتابة" مع "فحوى هذا الاتصال" إلى المحرك، وبعد ذلك يعالج محرك البحث البيانات الواردة من المستخدم، ويُرجع له قائمة من المواقع [ويتم كل هذا في شكل إلكتروني] (bozorgchami). أما أصحاب وجهة النظر الثانية ، فيرون أن هذا

القانون معني بحماية الاتصالات بين المستخدمين وبعضهم البعض، وليس لحماية استفسارات المستخدمين على الإنترنت، لذا لا ينطبق على محركات البحث ومصطلحات البحث (Erickson and Bankston, 2006). وهناك أيضًا قانون كاليفورنيا المعروف باسم California Online Privacy Protection Act of 2003 . وهو موجه أساسًا إلى المواقع التجارية على الإنترنت، التي تجمع المعلومات الشخصية عن مواطني كاليفورنيا (Burke, 2006).

يتبين لنا مما سبق أن القوانين الموجودة ، غير موجهة أساسًا لحماية خصوصية البحث على الإنترنت، لذا فهي لا توفر الحماية اللازمة لها. مما يعني ضرورة استحداث ووضع وصياغة قوانين وتشريعات جديدة تعمل على حماية تلك الخصوصية. وهناك نوعان من القوانين والتشريعات ينبغي وضعهما:

1/1/3 وضع قوانين لتحديد الضوابط اللازمة للوصول إلى سجلات بحث المستخدمين:
ينبغي وضع القوانين والتشريعات التي توضح متى وكيف يتم السماح للجهات الحكومية بالوصول إلى البيانات المسجلة عن أبحاث المستخدمين في محركات البحث، وبدون ذلك سيكون كل شخص مشتبهًا به (Duberman and Beaudet, 2000). كما أن السماح بمذكرات الاستدعاء الحكومية لبيانات البحث [بدون قيود]، يمكن أن يؤدي على المدى الطويل إلى مزيد من التطفل الحكومي على خصوصية مستخدمي الإنترنت (bozorgchami). وعلى تلك القوانين أيضًا تحديد ضوابط حصول الأفراد العاديين على تلك البيانات، ضمن القضايا الجنائية والمدنية.

2/1/3 وضع قوانين لضمان التزام محركات البحث بخصوصية الباحثين:
ينبغي وضع القوانين والتشريعات، التي تبين الحدود المسموح لمحركات البحث بالتعامل من خلالها مع خصوصية الباحثين، من حيث: أنواع المعلومات المسموح للمحركات بجمعها، والفترات الزمنية المسموح بالاحتفاظ فيها بتلك البيانات، ومتى ومع من وتحت أية قيود يمكن للمحرك تقاسم تلك البيانات مع أطراف أخرى، ..... بالإضافة إلى وضع عقوبات رادعة لمحركات البحث التي تنتهك خصوصية الباحثين وتتهاون فيها.

2/3 دور محركات البحث:
هناك الكثير من الإجراءات ينبغي على محركات البحث القيام بها، ومنها:

1/2/3 وضع سياسات الخصوصية:
ينبغي على محركات البحث، وضع سياسات خصوصية تحقق التوازن بين مطالب سوق الإعلانات واحتياجات خصوصية المستخدمين. ويشتمل هذا على وضع معايير وسياسات جديدة تأخذ الخصوصية في الاعتبار من البداية

(Center for Democracy Technology, 2007). وينبغي مراعاة الوضوح والبساطة عند صياغة تلك السياسات، كما ينبغي الإعلان بصورة جيدة عنها، مثل: وجودها على الصفحة الرئيسة للمحرك، أو وجود رابط Link يحتوي على كلمة "خصوصية" على الصفحة الرئيسة، على أن يتم تمييزه من خلال كتابته بحروف أكبر من، أو تساوي في الحجم النص المجاور لها، أو بنوع خط مختلف، أو لون مختلف. بالإضافة إلى توضيح كيفية إبلاغ المستخدمين بأية تغييرات جوهرية تحدث في تلك السياسة، وإدراج تاريخ فعالية السياسة (..... Business and Professions).

2/2/3 عدم تسجيل أية معلومات عن الأبحاث:
ينبغي عدم تسجيل أية معلومات عن الأبحاث يمكن أن تُربط بالمستخدمين. وبعد انتهاء جلسة العمل، ينبغي ألا يتم تخزين بيانات يمكن ربطها بمستخدم معين، إلا إذا تم إعلام هذا المستخدم بشكل واضح، والحصول على موافقته باحتفاظ المحرك بالبيانات الضرورية لتقديم خدمة معينة "الأبحاث المستقبلية على سبيل المثال" (Resolution on Privacy Protection and Search Engines, 2006).

3/2/3 الحصول على موافقة من المستخدمين، قبل الحصول على المزيد من الإعلانات على أساس عبارات البحث التي يجرونها.

4/2/3 عدم الاحتفاظ بالبيانات الشخصية عن المستخدمين لمدة تزيد عن ستة أشهر، وفي حالة قيام محرك البحث بالاحتفاظ بالبيانات الشخصية لمدة أطول من ذلك، لأغراض الأمن أو لمنع الغش، فإن هذا الإبقاء ينبغي أن يكون له ما يبرره (EU Panel: Delete Search Info Sooner, 2008).

5/2/3 عدم استخدام بيانات المستخدمين إلا للأغراض التي جُمعت من أجلها (Eecke and Truyens, 2008).

6/2/3 وصف الإجراءات التي يستطيع المستخدمون من خلالها الوصول إلى البيانات المخزنة في المحرك عن أبحاثهم، والسماح لهم بحذفها (Cooley, 2004).

7/2/3 ابتكار أساليب جديدة –بالتعاون مع الباحثين والأكاديميين- لتحسين نوعية نتائج البحث، ومنع الغش وغير ذلك مما يلبي احتياجات التجارة دون ربط الأبحاث بالمستخدمين.

8/2/3 توفير الوسائل اللازمة للحفاظ على أمن قواعد البيانات التي يتم فيها تخزين البيانات عن المستخدمين، حتى لا يخترقها قراصنة الإنترنت (Center for Democracy Technology, 2007).

9/2/3 التأكيد على الشركات التي تعمل مع محركات البحث -مثل المعلنين- ضرورة احترام خصوصية المستخدمين (Electronic Frontier Foundation, 2008).

10/2/3 تقديم معلومات كافية عن الغرض من ملفات تعريف الارتباط، وكيف يمكن الوصول إليها، ومنعها، والفترة التي ستبقى مثبتة فيها على حاسب المستخدم (Eecke and Truyens, 2008).

3/3 دور المستخدم:

في ظل عدم وجود قوانين كافية لحماية خصوصية البحث على الإنترنت، وعدم ضمان احترام محركات البحث لتلك الخصوصية، فإن العبء الأكبر يقع على عاتق المستخدم نفسه. حيث ينبغي عليه اتخاذ عدة خطوات جادة حتى يستطيع البحث على الإنترنت، وهو آمن قدر المستطاع. ومن الإجراءات التي تقترحها الباحثة في هذا الصدد:

1/3/3 قراءة سياسات الخصوصية في محركات البحث:

ينبغي على المستخدم قراءة سياسات الخصوصية في مواقع محركات البحث بعناية، حتى يتأكد من أنه موافق عليها. فبعض السياسات قد تكون غير واضحة، أو غامضة، أو يصعب فهمها، أو قد يشير إلى علاقات غير واضحة مع شركات غير محددة. ولأن محركات البحث تدخل من حين لآخر العديد من التغييرات على سياساتها دون إشعار، فيجب على المستخدم أن يقرأ تلك السياسات بانتظام لمعرفة التحديثات أو التغييرات التي طرأت عليها. وقد تكون هناك حاجة أيضًا لقراءة البنود والشروط Terms and Conditions التي يضعها المحرك، أو ما يعادلها، لأنها قد تغير ما جاء في سياسة الخصوصية. فعلى سبيل المثال، قد تنص سياسة الخصوصية بوضوح على أن تقاسم المعلومات لا يتم دون إذن المستخدم، ولكن اتفاقية التسجيل لخدمة ما من خدمات المحرك، تُصرح بأنه ومن خلال التسجيل، فإن المستخدم يعطي تلقائيًا الإذن بتقاسم المعلومات المخزنة في قواعد بيانات المحرك عنه (Duberman and Beaudet, 2000).

2/3/3 عدم وضع معلومات شخصية مميزة في مصطلحات البحث:

ينبغي ألا يبحث المستخدم من خلال الإنترنت عن اسمه، أو عنوانه، أو رقم بطاقته الائتمانية، أو رقم ضمانه الاجتماعي، أو غير ذلك من المعلومات الشخصية. فهذه الأنواع من الأبحاث يمكنها رسم خارطة تؤدي مباشرة إلى عتبة داره. ويمكن أيضًا أن تعرضه لسرقة الهوية identity، وغير ذلك من انتهاكات الخصوصية. وإذا كان المستخدم يريد القيام

بمثل هذه الأبحاث، فعليه القيام ببقية الاقتراحات التالية، أو إجراء بحثه هذا من حاسب آلي مختلف عن الذي يستخدمه عادة في البحث (Eckersley...[et al], 2006).

3/3/3 عدم استخدام محرك البحث المسجل لديه المستخدم، أو المشترك في إحدى خدماته:

تعطي محركات البحث في بعض الأحيان الفرصة لتكوين حساب شخصي وتسجيل دخول. وبالإضافة إلى ذلك، قد تقدم خدمات أخرى، فعلى سبيل المثال يقدم Google خدمات مثل Gmail، و Google Chat ؛ ويقدم MSN خدمات مثل Hotmail، و MSN Messenger. وعندما يسجل المستخدم للدخول إلى محرك البحث أو واحدة من تلك الخدمات، فيمكن للمحرك ربط أبحاث المستخدم معًا، وربطها كذلك بحسابه الشخصي. لذا إذا كان لدى المستخدم حساب مع خدمات Google مثل Gmail، و Google Chat، وإذا كان لديه حساب مع خدمات MSN مثل Hotmail، و MSN Messenger، فعليه ألا يبحث باستخدام محرك البحث Google و Live Search على التوالي. وإذا كان يجب على المستخدم استخدام محرك البحث والبريد الإلكتروني (أو غيرها من الخدمات) لشركة واحدة، سيكون من الصعب حماية خصوصية بحثه. وسوف يحتاج إلى القيام بأحد الإجراءين الآتيين:

أ. تثبيت install متصفحين مختلفين من متصفحات الإنترنت، وذلك لفصل أنشطة البحث الخاصة به عن حساباته الأخرى. فعلى سبيل المثال، عليه استخدام المتصفح Mozilla Firefox للبحث خلال Yahoo، واستخدام المتصفح Internet Explorer للوصول إلى البريد الإلكتروني وغيره من خدمات Yahoo. مع مراعاة الاقتراحات [من 3 /2/3 إلى 6/3/3] مع واحد من المتصفحين على الأقل.

ب. عند استخدام Google وخدماته، يمكن استخدام متصفح Mozilla Firefox والبرنامج المساعد CustomizeGoogle، (يمكن الحصول عليه من خلال http://www.customizegoogle.com/). ويجب على المستخدم تذكر الخروج من متصفحه بعد استخدام Gmail وقبل استخدام محرك بحث Google. بالإضافة إلى ذلك، عليه التأكد من عدم اختياره لخيار "تذكرني على هذا الكمبيوتر" عندما يقوم بتسجيل الدخول إلى خدمة Google. أما إذا كان يستخدم متصفح غير Firefox، فيمكنه استخدام GoogleAnon bookmarklet ، (يمكن الحصول عليه من http://www.imilly.com/google-cookie.htm). وسيحتاج المستخدم إلى ترك المتصفح في كل مرة ينتهي فيها مع خدمة Google. (Eckersley...[et al], 2006)

4/3/3 حذف ملفات تعريف الارتباط ومنعها:

إذا نفذ المستخدم الخطوات المذكورة في [2/3/3 و3/3/3]، فإن تاريخ البحث الخاص به لم يعد يشتمل على معلومات شخصية مميزة له. ومع ذلك، لا يزال محرك البحث الذي يستخدمه قادر على ربط أبحاثه معًا باستخدام ملفات تعريف الارتباط وعنوان بروتوكول الإنترنت. والاقتراح رقم [4/3/3] سوف يمنع تعقب المستخدم باستخدام ملفات تعريف الارتباط، بينما الاقتراحان [3/3/ 5 و 6/3/3] سوف يمنعان التعقب القائم على تتبع عنوان بروتوكول الإنترنت. ومن

الأفضل إتباع الاقتراحات [من 3/3/3 إلى 6/3/3] معًا، لأن الفائدة تكون أقل إذا منع المستخدم ارتباط أبحاثه معًا بطريقة ما، إذا كان يمكن ربطها بطريقة أخرى.

1/4/3/3 حذف ملفات تعريف الارتباط:

يمكن للمستخدم حذف ملفات تعريف الارتباط بأكثر من طريقة:

1/1/4/3/3 الطريقة اليدوية:

يمكن للمستخدم حذف ملفات تعريف الارتباط المثبتة على حاسبه الآلي يدويًا، وعليه الانتباه أن الحذف اليدوي يتطلب منه إعادة الحذف يدويًا بشكل مستمر؛ لأن محركات البحث سوف تثبت ملفات تعريف ارتباط جديدة على حاسب المستخدم، كلما حذف ملفات تعريف الارتباط القديمة. والخطوات الآتية والشكل رقم (2) يوضحان كيفية حذف ملفات تعريف الارتباط يدويًا:

أ. من قائمة "أدوات" Internet Explorer، اختر "خيارات إنترنت".

ب. اضغط على "عام"، ثم على علامة التبويب "حذف محفوظات الاستعراض".

ج. اختر حذف ملفات تعريف الارتباط.

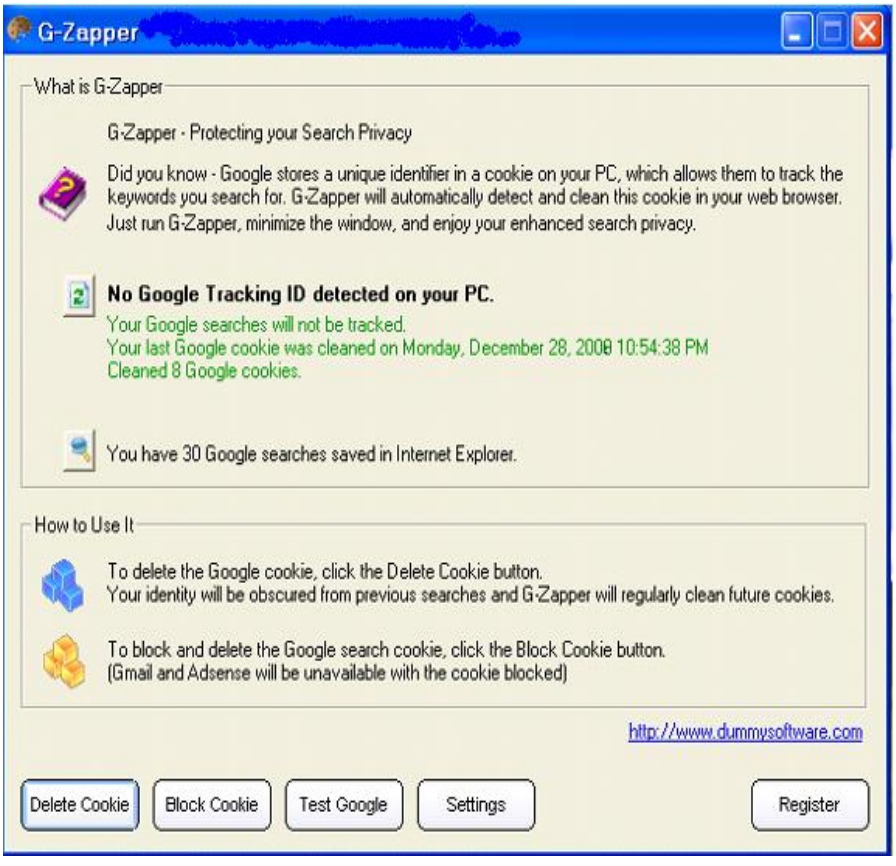
شكل رقم (2)

حذف ملفات تعريف الارتباط يدويًا

2/1/4/3/3 الطريقة الآلية:

تتطلب الطريقة السابقة جهدًا مستمرًا من المستخدم، لأنها طريقة يدوية كما سبق القول، لذا يُفضل استخدام برمجيات لتقوم بهذه العمليات بشكل آلي، ومن أمثلة هذه البرمجيات برمجيةG-Zapper. وبمجرد تثبيت المستخدم لهذه البرمجية، فإنها تقرأ ملفات تعريف الارتباط الخاصة بـGoogle المثبتة installed على حاسبه الآلي، وتعرض تاريخ تثبيتها، وتحدد المدة التي تم خلالها تعقب أبحاث المستخدم، وتعرض الأبحاث التي أجراها باستخدام Google. وهي تسمح بشكل

آلي للمستخدم حذف تلك الملفات أو منعها تمامًا من التثبيت في المستقبل [انظر الشكل رقم (3)]. وتصلح هذه البرمجية أيضًا للاستخدام مع المحركات الأخرى مثل Yahoo, MSN, Ask, وغيرها (K.Soft).



شكل رقم (3)

حذف ملفات تعريف الارتباط آليًا

موقع برمجية G-Zapper على الإنترنت:

http://www.dummysoftware.com/gzapper.html

2/4/3/3 منع ملفات تعريف الارتباط:

من الأفضل منع جميع ملفات تعريف الارتباط [يمكن الاستفادة من برمجيةG-Zapper في هذا المجال] ، وذلك من منظور حماية الخصوصية. ولكن لأن هذه الملفات ضرورية للوصول إلى العديد من المواقع، قد يكون الأكثر ملاءمة - وإن كان أقل حماية للخصوصية- السماح بـــملفات تعريف الارتباط في "جلسات العمل session cookies" قصيرة الأجل. وتبقى تلك الملفات فقط ما دام متصفح المستخدم مفتوحًا؛ ولذلك، إذا أغلق المستخدم متصفحه، ثم أعاد فتحه مرة

أخرى، وعاد بعد ذلك إلى محرك البحث، فإن المحرك لن يكون قادرًا على ربط أبحاثه الحالية مع السابقة عن طريق ملفات تعريف الارتباط الخاصة به. وعلى المستخدم الانسحاب من المتصفح مرة واحدة في اليوم على الأقل، ولكن من الناحية المثالية عليه الانسحاب بعد كل زيارة إلى موقع محرك البحث. ويمكن استخدام الخطوات الآتية [انظر أيضًا الشكل رقم (4)] للسماح فقط بـــملفات تعريف الارتباط في جلسات العمل "session cookies"، وذلك مع متصفح Microsoft Internet Explorer (Eckersley...[et al], 2006):

أ. من قائمة "أدوات" Internet Explorer، اختر "خيارات إنترنت".

ب. اضغط على "خصوصية"، ثم على علامة التبويب "خيارات متقدمة".

ج. اختر تجاوز المعالجة التلقائية لملفات تعريف الارتباط.

د. اختر "منع" في كل من "ملف تعريف الموقع الحالي" و "ملفات تعريف الموقع غير المستخدم حاليًا].

هـــ. اختر "السماح بملفات تعريف الارتباط في جلسات العمل دومًا".

شكل رقم (4)

السماح بـــملفات تعريف الارتباط في جلسات العمل

5/3/3 تغيير عنوان بروتوكول الإنترنت:

عند اتصال المستخدم بالإنترنت يقوم مزود خدمة الإنترنت ISP بتسجيل "عنوان بروتوكول الإنترنت" الخاص بحاسب هذا المستخدم. ويستطيع مقدم خدمة البحث وغير ذلك من الخدمات التي يتفاعل معها المستخدم على الإنترنت، استخدام هذا الرقم لربط جميع أبحاث المستخدم معًا. وخلافا لملفات تعريف الارتباط، فإن "عنوان بروتوكول الإنترنت" لا يتبع الحاسب أينما يذهب؛ فعلى سبيل المثال، سيكون للحاسب عنوان بروتوكول مختلف، مع كل شركة اتصالات يتم استخدامها للوصول إلى الإنترنت. وإذا كان مزود خدمة الإنترنت لدى المستخدم، يعطيه عنوان بروتوكول إنترنت متغير بشكل ديناميكي لحاسبه، أو كان المستخدم يتصفح الإنترنت من حاسب المكتب، والذي يعمل من وراء الجدار الناري firewall، فإن هذا القلق يخف.

ولكن، إذا كان لدى المستخدم عنوان بروتوكول إنترنت متغير "عنوان بروتوكول إنترنت ديناميكي dynamic IP address" على اتصال النطاق العريض broadband connection، فسيحتاج إلى إغلاق المودم modem الخاص به بشكل متكرر، لجعل العنوان يتغير. وأفضل طريقة للقيام بذلك هي إغلاق المودم عند انتهاء المستخدم من العمل على حاسبه، وتركه مغلقًا طوال الليل. وعلى الجانب الآخر، إذا كان "عنوان بروتوكول الإنترنت" لدى المستخدم لا يتغير، "عنوان بروتوكول إنترنت ثابت static IP address"، فسيحتاج بالتأكيد إلى استخدام برمجيات لإخفاء الهوية لإبقاء عنوانه خاصًا ؛ انظر الاقتراح رقم [6/3/3]. (Eckersley...[et al], 2006)

6/3/3 استخدام وكلاء الإنترنت web proxies وبرمجيات إخفاء الهوية:

لإخفاء عنوان بروتوكول الإنترنت الخاص بالمستخدم من مواقع الويب التي يزورها أو الحاسبات الأخرى التي يتواصل معها على الإنترنت، يمكنه استخدام أجهزة الحاسبات الأخرى كبدائل proxies؛ حيث ترسل هذه الحاسبات اتصال المستخدم إلى الوكيل، ويقوم الوكيل بإرسال الاتصال إلى المرسل إليه، الذي يستجيب للوكيل، وأخيرًا، فإن الوكيل يعيد الاستجابة إلى جهاز الحاسب الخاص بالمستخدم. وقد يبدو الأمر معقدًا، لكن هناك أدوات متاحة يمكن أن تفعل هذا نيابة عن المستخدم بسهولة إلى حد ما. ومن أمثلتها "Anonymizer's Anonymous Surfing" (Eckersley...[et al], 2006)، الذي يقوم بإخفاء عنوان برتوكول الإنترنت الحقيقي للمستخدم، ويسمح بتشفير بياناته (Go Trusted.com, 2008). ومن برمجيات إخفاء الهوية أيضًا "Tor"، وهي برمجية تقوم بتشفير حركة المرور الخاصة بالمستخدم، وبعد ذلك ترسلها على الإنترنت من خلال سلسلة من الحاسبات يتم اختيارها عشوائيا، ومن ثم تحجب مصدر طلبات المستخدم ومسارها. وهي تتيح للمستخدم التواصل مع جهاز حاسب آخر على الإنترنت دون أن يعرف ذلك الحاسب، أو الحاسبات في المنتصف من هو(Eckersley...[et al], 2006). وتحمل هذه البرمجيات خطورة لأنها تخفي هوية المجرمين على الإنترنت، إلا أن منتجي تلك البرمجيات يرون أن المجرمين لديهم وسائلهم التي يستخدمونها لارتكاب جرائمهم، وإخفاء هويتهم أثناء تواجدهم على الإنترنت، وربما تكون تلك الوسائل أفضل من "Tor"، وأن "Tor" يهدف إلى حماية

الأشخاص العاديين الذين يتبعون القانون، ويرغبون في الحفاظ على خصوصيتهم (Tor, 2008 A). وTor ليس مثاليًا، مثله في ذلك مثل نظم إخفاء الهوية، لذا على المستخدم عدم الاعتماد على هذه البرمجية بمفردها، إذا كان يحتاج إلى سرية شديدة (Tor, 2008 B).

7/3/3 استخدام محركات بحث آمنة:

1/7/3/3 محرك البحث Ixquick :

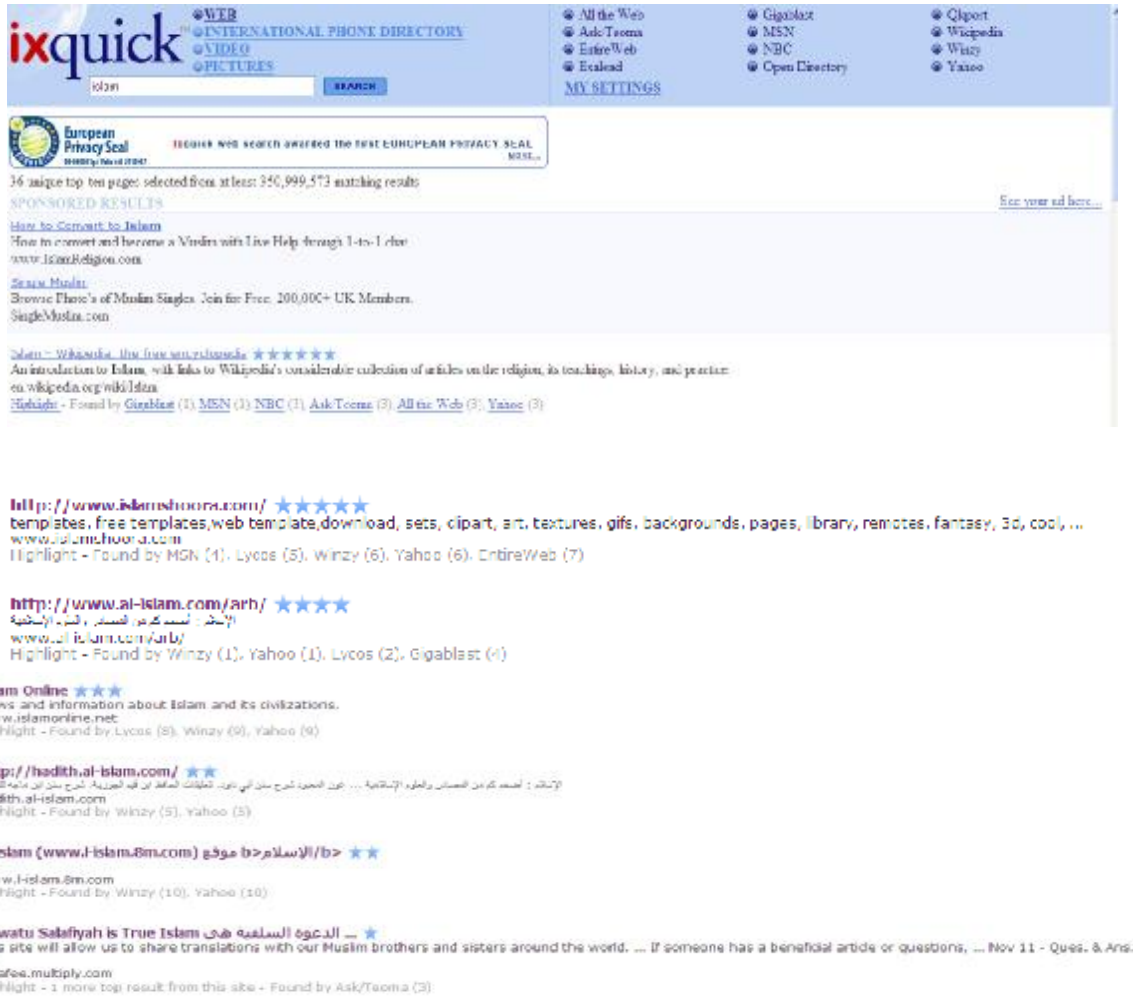
تأسس Ixquick في عام 1998م، ومنذ ذلك الحين أظهر نموًا قويًا، فقد عالج في عام 2004م ما يزيد على 120 مليون بحث. وفاز بالعديد من الجوائز، تشتمل على:

- Best Metasearch 2000 Search Engine Watch Awards
- A "great meta search engine" 2002 (Search Engine Watch)
- Top Choice" for Metasearch 2004 (Search Engine Watch)
- Best Metasearch 2005 by Pandia. Etc.

كما حصل عام 2008م، على أول جائزة رصدها European Privacy Seal لمنتجات ICT والخدمات المعتمدة على تكنولوجيا المعلومات. وهي تُمنح للالتزام بقوانين وتشريعات الاتحاد الأوروبي حول أمن البيانات وخصوصيتها (EuroPriSe, 2008).

ولا يعني استخدام Ixquick التخلي عن محركات البحث الأخرى؛ فهو محرك عن المحركات metasearch engine، يوفر الخصوصية الكاملة للمستخدمين أثناء بحثهم؛ لأنه يعمل كوكيل proxy، أي أن عناوين بروتوكول الإنترنت الخاصة بالمستخدمين لا يتم كشفها لمحركات البحث الأخرى. ويبحث Ixquick في العديد من محركات البحث الشهيرة، مثل: Yahoo، وGigablast ، وAsk/Teoma، وOpen Directory، وMSN، وAll the Web والعديد من المحركات الأخرى في نفس الوقت. وهذا له ميزتان؛ فالجمع بين هذه المحركات يقدم تغطية أكبر للإنترنت، أكثر مما يستطيع محرك واحد أن يفعل، ويؤدي إلى التخلص من التلاعب التجاري لبعض المحركات. كما أن هذا المحرك يقدم الحد الأدنى من الإعلانات ذات الصلة بالنتائج، ويشير إليها بوضوح في أعلى الصفحة، وهي تقتصر على ثلاثة فقط. وبالإضافة إلى تلك المزايا، فإن Ixquick يحذف عناوين بروتوكول الإنترنت الخاصة بالمستخدمين خلال 48 ساعة منذ يونيو 2006م، مما يوفر الخصوصية الكاملة، كما أنه ألغى استخدام الهوية الفريدة من ملفات تعريف الارتباط (Ixquick, 2008)، أما البيانات غير الشخصية فيحذفها خلال 14 يومًا (EuroPriSe, 2008).

وتتلخص طريقة عمل Ixquick في أنه يسترجع نتائج البحث من محركات البحث الأخرى. وهو يستخدم نظام النجوم star system لترتيب نتائجه، من خلال منح نجمة واحدة لكل نتيجة تم استرجاعها من محرك بحث آخر. لذا تكون النتائج الأولى هي النتائج التي تم استرجاعها من أكبر عدد من محركات البحث (Alert: Keep Your Internet Searches Private, 2006)، كما أنه يذكر المحركات التي تم استرجاع تلك النتائج منها. ويبين الشكل رقم (5) أشكال نتائج البحث المسترجعة باستخدام هذا المحرك.



الشكل رقم (5)

أشكال نتائج البحث المسترجعة باستخدام Ixquick

موقع محرك البحث Ixquickعلى الإنترنت:

http://www.ixquick.com/

2/7/3/3 محرك البحث Privacy Finder :

يعزز محرك البحث "Privacy Finder" الخصوصية؛ لأنه يحتفظ ببيانات المستخدم لمدة أسبوع واحد فقط، وبعدها يتم حذف كل البيانات باستثناء مصطلحات البحث، التي يتم الاحتفاظ بها للأغراض البحثية، ولا يمكن بأي حال ربطها مرة أخرى بفرد بعينه أو بحاسبه الآلي. ولا يستخدم هذا المحرك ملفات تعريف الارتباط إلا إذا كان المستخدم قد اختار خيار

الخصوصية "مخصص custom"، لتعرف المعايير التي اختارها المستخدم، وهذه الملفات لا تُستخدم لتعقب سلوكه أو تحديد هويته (Usable Privacy and Security Laboratory). كما أن Privacy Finder ، يقدم ميزة مهمة أخرى تميزه عن غيره من محركات البحث، حيث يمكن للمستخدم معرفة ما ستفعله المواقع مع بياناته من البداية، لذا يتمكن من تصفح الإنترنت وهو يحمي خصوصيته.

وتتلخص طريقة عمل هذا المحرك، في الخطوات الآتية:

1. إدخال المستخدم عبارات البحث التي يرغب في البحث عنها.
2. تحديد المستخدم محرك البحث الذي يرغب البحث فيه "Yahoo أو Google".
3. تحديد المستخدم خياراته للخصوصية (المنخفضة أو المتوسطة أو المرتفعة ، أو مخصص custom) [انظر الشكل رقم(6)]. ويحذر الخيار "منخفض low" المستخدم من المواقع التي تقوم بجمع المعلومات الطبية والصحية واستخدامها لأغراض أخرى غير الوفاء بطلبه، أو التي قد لا تسمح له بحذف بياناته من قوائمها البريدية/ التسويقية. ويشتمل الخيار "متوسط medium" على كل الخصائص الواردة في الخيار "منخفض"، ولكن مع إضافة سمات لتحذير المستخدم من المواقع التي تتشارك في معلوماته المالية مع أطراف ثالثة، أو التي تتقاسم معلوماته الشخصية مع أطراف ثالثة، أو التي لا تسمح له برؤية البيانات التي جمعتها عنه. ويشتمل الخيار "مرتفع high" على كل الخصائص الواردة في الخيار "متوسط"، ولكن مع إضافة سمات لتحذير المستخدم من المواقع التي تجمع المعلومات المالية الخاصة به لأغراض أخرى غير الوفاء بطلبه، أو التي تحلل معلوماته الشخصية، أو التي تقوم بجمع أو تشارك معلوماته غير الشخصية لأغراض أخرى غير الوفاء بطلبه. أما الخيار "مخصص custom" فيعطي المستخدم فرصة اختيار المعايير التي يريدها (Privacy Finder).

الشكل رقم (6)

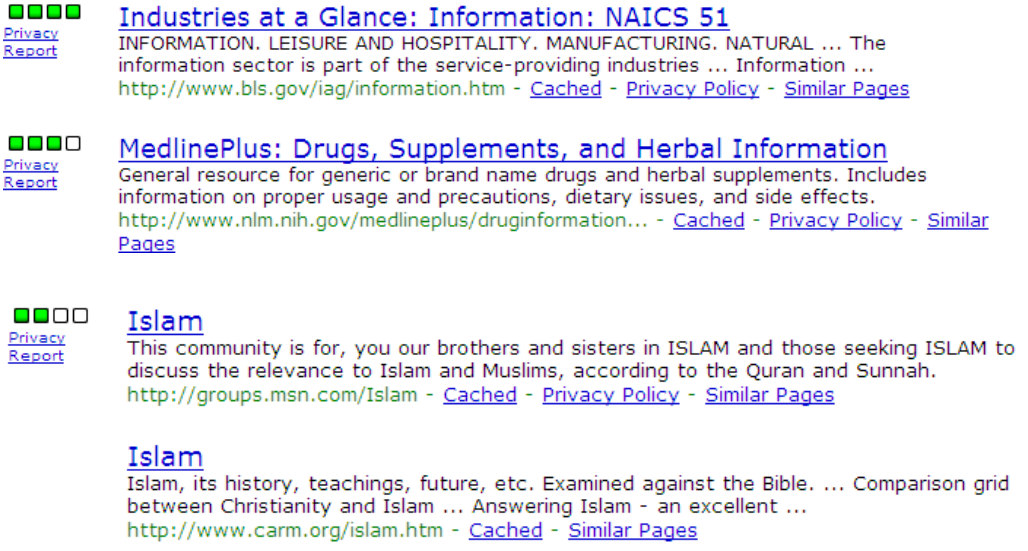
Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

---

4. قيام "Privacy Finder"، بالبحث في محرك البحث الذي اختاره المستخدم، والتحقق من كل موقع تم استرجاعه في محاولة لتحديد ما إذا كانت لديه سياسة خصوصية في شكل "P3P ". والجدير بالذكر أن Platform for Privacy Preferences Project (P3P)، هو معيار standard يسمح لمواقع الويب بإنشاء نسخة (XML) من سياسة الخصوصية بها، وتستطيع المواقع بهذا التعبير عن ممارسات الخصوصية لديها في شكل معياري، مما يسمح باسترجاعها وتفسيرها آليًّا بسهولة بواسطة وكلاء المستخدم user agents . ويسمح ذلك للوكلاء بإعلام المستخدمين بالمعلومات عن ممارسات الموقع (في أشكال قابلة للقراءة الآلية والبشرية)، وإلى أتمتة عملية صنع القرار على أساس هذه الممارسات عند الحاجة. وبالتالي لا حاجة للمستخدمين لقراءة سياسات الخصوصية في كل المواقع التي يزورونها (W3C, 2007). والجدير بالذكر أنه ورغم توفير أسلوب "P3P " لآلية تقنية للتأكد من أن المستخدم يتم إعلامه عن سياسات الخصوصية للموقع قبل أن يقدم معلوماته الشخصية إليه، فإنه لا يوفر الآلية التقنية للتأكد من أن تلك المواقع تتصرف وفقًا لسياساتهم التي ذكروها (W3C, 2006).

5. تقييم "Privacy Finder" لسياسات الخصوصية المقروءة آليًّا "P3P " في المواقع المسترجعة، وفقًا لخيارات الخصوصية التي حددها المستخدم. ويتم استخدام مقياس مكون من أربعة إطارات خضراء (■■■■) تشير إلى تماثل موقع الويب مع خيار المستخدم للخصوصية. والمواقع التي لا تتوافق مع بعض أو كل خيارات المستخدم، ستحصل على إطارات خضراء عددها أقل من أربعة. وعدد الإطارات الخضراء المفقودة يتناسب مع عدد التعارض بين سياسة خصوصية الموقع وخيار المستخدم. ويعني غياب مقياس الخصوصية، عدم وجود سياسة خصوصية صالحة للقراءة آليًّا في الموقع (Privacy Finder) ، وقد لاحظت الباحثة أن عددًا كبيرًا من المواقع لا يوجد أمامه مقياس الخصوصية، ويعني هذا أن غالبية مواقع الويب لا تستخدم معيار "P3P ".

6. إظهار نتائج البحث للمستخدم: يتم في النهاية إظهار نتائج البحث للمستخدم، وبجوار كل موقع مقياس الخصوصية، ممثلا لمدى توافق هذا الموقع مع خيار المستخدم للخصوصية، في حالة وجود سياسة "P3P "، أو غائبًا في حالة عدم وجود سياسة "P3P ". [انظر الشكل رقم (7)]. وعند رغبة المستخدم في معرفة التعارض الموجود بين خيار الخصوصية الذي حدده وبين المواقع الظاهرة في نتائج البحث، فعليه الوقوف بالفأرة على مقياس الخصوصية، فتُعرض له قائمة قصيرة توضح له ذلك. أما الضغط على المقياس، فسوف يجلب له موجزًا لسياسة خصوصية الموقع، ومعلومات عن التعارض، كما يتيح له رابطًا يؤدي إلى سياسة الخصوصية الكاملة للموقع. ويمكنه أيضًا الوصول للسياسة الكاملة من غير الضغط على المقياس حيث يوردها المحرك مع البيانات عن الموقع والرابط المؤدي إليه.



الشكل رقم (7)

نتائج البحث في محرك البحث Privacy Finder

موقع محرك البحث Privacy Finder على الإنترنت:

http://www.privacyfinder.org/

8/3/3 وفي الختام، ينبغي أن يحافظ المستخدم بشكل مستمر على معرفته بالتطورات الجديدة في عالم التكنولوجيا، والبرمجيات، والقوانين، .... التي تؤثر في قضايا الخصوصية (Duberman and Beaudet, 2000).

4. النتائج:

تتمثل أهم النتائج التي تم التوصل إليها عن طريق الدراسة الحالية فيما يلي:

- هناك نوعان أساسيان من المعلومات التي يتم جمعها عن المستخدم في محركات البحث، هما: المعلومات الشخصية، والمعلومات غير الشخصية. والمعلومات الشخصية، هي المعلومات التي يتم جمعها عن شخص ما، وتتيح الاتصال المباشر به. والمعلومات غير الشخصية، وهي المعلومات التي لا يمكن أن تعود في حد ذاتها إلى فرد بعينه.
- من الصعب على محرك البحث تحديد هوية مستخدم معين. إلا أن الحالة تختلف تمامًا عندما يكون المستخدم مُسجلا في المحرك، أو اشترى شيئًا أثناء تواجده على موقعه. حيث يمكن للمحرك في هذه الحالة، ربط المصطلحات

التي بحث بها المستخدم عن المعلومات، بأي معلومات محددة للشخصية، مما يمكن المحرك من تحديد هوية مستخدم معين.

- تتزايد المخاوف من جمع محركات البحث للبيانات عن المستخدمين، لعدة أسباب منها: إمكانية وصول الجهات الحكومية لتلك البيانات، واحتمال إعلان المحركات عن البيانات، أو بيعها، أو تقديمها للشركات الأخرى عند حدوث اندماج بينها، وإمكانية الرصد التفصيلي لحياة الأفراد، وتعرض البيانات للسرقة أو الهجوم.
- تلجأ محركات البحث إلى أساليب عدة لجمع البيانات عن المستخدمين، من أهمها: المستخدم نفسه، وعنوان بروتوكول الإنترنت، وملفات تعريف الارتباط، وعدادات الشبكة، وشريط الأدوات ومُسرِّع الويب، وسجلات مركز الخدمة، وتاريخ البحث، والمواقع التابعة.
- تتنوع الأسباب التي تدعو محركات البحث لجمع المعلومات من المستخدمين أو عنهم، فهناك أسباب تتعلق بالمحركات نفسها ورغبتها في تحسين خدماتها الحالية وتقديم خدمات جديدة، وتخصيص المحتوى والإعلانات للحصول على الأموال، وحماية ممتلكاتها وموظفيها. ومنها ما يتعلق بالمستخدم نفسه، مثل الاتصال به والوفاء بطلباته. ويمكن القول بصفة عامة، أن الاحتفاظ بالمعلومات عن المستخدمين هي لصالح المحرك بالدرجة الأولى، ولصالح المستخدم بالدرجة الثانية.
- محركات البحث كانت في البداية تحتفظ بالبيانات عن الأبحاث التي تُجرى خلالها لفترات غير محدد، ثم حددت فترات أقصر للاحتفاظ بالبيانات فيما بعد، حتى تتجنب النقد الموجه لها . إلا أن المهتمين بالخصوصية، يرون أن تلك الفترات ما زالت فترات طويلة.
- تتنوع ممارسات محركات البحث، فيما يتعلق بحذف بيانات البحث، فهناك محركات تحذف عناوين بروتوكول الإنترنت ورقم هوية ملفات تعريف الارتباط بشكل كامل، وهناك محركات تحذف هذه الأرقام حذفًا جزئيًا. أما نص الاستفسار نفسه، فهناك محركات تحتفظ فقط بإحصاءات مجمعة عن تكرار الاستفسار، وهناك محركات تحذفه بالكامل، وهناك محركات تبقي عليه ولا تحذفه.
- يمكن لمحركات البحث أن تتشارك في المعلومات التي تجمعها من المستخدمين أو عنهم مع جهات أخرى، دون موافقة المستخدم.
- غالبية المحركات لا تتيح للمستخدم، إمكانية حذف بيانات بحثه من خوادمها.

وتوضح النتائج السابقة بصفة عامة، أن غالبية محركات البحث لا تحافظ على خصوصية البحث للمستخدم، فهي لا تتيح له الفرصة لتحديد المعلومات التي ستُجمَعُ منه أو عنه، كما أنها تكشف عن هذه المعلومات لأطراف أخرى دون موافقة منه.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 18، مارس 2009

---

5. التوصيات:

يمكن توجيه التوصيات إلى ثلاث فئات رئيسة، هي الدول، ومحركات البحث، والمستخدم نفسه:

1/5 الدول:

ينبغي على الدول وضع قوانين لتحديد الضوابط اللازمة للوصول إلى سجلات بحث المستخدمين، وقوانين لضمان التزام محركات البحث بخصوصية الباحثين وحماية هذه الخصوصية.

2/5 محركات البحث:

على محركات البحث القيام بالعديد من الجهود، حتى تبرهن على احترامها لخصوصية المستخدمين، ومنها: وضع سياسات خصوصية تحقق التوازن بين متطلبات سوق الإعلانات واحتياجات خصوصية المستخدمين، ومراعاة الوضوح والبساطة عند صياغتها، والإعلان الجيد عنها. وعدم تسجيل أية معلومات عن الأبحاث يمكن أن تُربط بالمستخدمين. والحصول على موافقة من المستخدمين، قبل الحصول على المزيد من الإعلانات على أساس عبارات البحث التي يجرونها، وقبل إتاحة البيانات عن أبحاثهم للغير. وعدم الاحتفاظ بالبيانات الشخصية عن المستخدمين لمدة تزيد عن ستة أشهر، وعدم استخدام بيانات المستخدمين إلا للأغراض التي جُمعت من أجلها، وتوفير الوسائل اللازمة للحفاظ على أمن قواعد البيانات التي يتم فيها تخزين البيانات عن المستخدمين حتى لا يخترقها قراصنة الإنترنت، وتقديم معلومات كافية عن الغرض من ملفات تعريف الارتباط، وكيف يمكن الوصول إليها، ومنعها، والفترة التي ستبقى مثبتة فيها على حاسب المستخدم، ...

3/5 المستخدم

ينبغي على المستخدم العمل على حماية خصوصيته أثناء البحث على الإنترنت، ومن التوصيات التي يمكن تقديمها له في هذا المجال: قراءة سياسات الخصوصية في محركات البحث باستمرار، وعدم وضع معلومات شخصية مميزة في مصطلحات البحث، وعدم استخدام محرك البحث المسجل لديه المستخدم، أو المشترك في إحدى خدماته. وحذف ملفات تعريف الارتباط ومنعها، وتغيير عنوان بروتوكول الإنترنت، واستخدام وكلاء الإنترنت web proxies وبرمجيات إخفاء الهوية، واستخدام محركات بحث آمنة، بالإضافة إلى ضرورة محافظته بشكل مستمر على معرفته بالتطورات الجديدة في عالم التكنولوجيا، والبرمجيات، والقوانين، .... التي تؤثر في قضايا الخصوصية.

المراجع:

(1) أحمد، فايزة دسوقي. (قيد النشر). سياسات الخصوصية في محركات البحث العربية والأجنبية: دراسة تحليلية مقارنة.

(2) Aggarwal, Gagan. (2005). Privacy protection and advertising in a networked world.- [Stanford?]: G. Aggarwal.- 123 p.
(3) Alert: Keep Your Internet Searches Private. (2006). Available at: http://www.privacyrights.org/ar/Ixquick.htm. Accessed at: 5/11/2008.
(4) And then there were four.- Available at: http://www.google-watch.org/bigbro.html. Accessed at: 25/10/2008.
(5) AOL. (2008 a). [Privacy Policy].- Available at: http://about.aol.com/aolnetwork/aol_pp . Accessed at: 1/10/2008.
(6) AOL. (2008 b). Search History.- Available at: http://search.aol.com/aol/recent?s_it=recentSearchMaint&&itag=0.1.1.&static=0&a=1&ro=1. Accessed at: 16/12/2008.
(7) Article 29 Data Protection Working Party. (2008). Opinion 1/2008 on data protection issues related to search engines.- 29 p. .- Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf. Accessed at: 2/10/2008.
(8) Ask. (2008 a). About AskEraser. Available at: http://sp.ask.com/en/docs/about/askeraser.shtml#12. Accessed at: 2/10/2008
(9) Ask. (2008 b). Privacy Policy for Ask.com.- Available at: http://about.ask.com/en/docs/about/privacy.shtml. Accessed at: 2/10/2008.
(10) bozorgchami, pouya. Googling away your privacy: Protecting online search inquiries from unwarranted state intrusion.- Available at: http://llr.lls.edu/student_symposium/40/Pouya%20Bozorgchami%20-%20Note.doc. Accessed at: 5/11/2008.
(11) Brandt, Daniel. (2002). We asked Google about privacy.- available at: http://www.google-watch.org/krane.html. Accessed at: 11/11/2008
(12) Brown, Andrew. (2006). They know all about you.- Available at: http://www.guardian.co.uk/world/2006/aug/28/usa.searchengines. Accessed at: 13/11/2008.
(13) Burke, Thomas R. (2006). Internet search terms: Embedded privacy issues.- The Privacy & Data Security Law Journal. vol. 1 (5).- pp.441-447. Available at: http://www.dwt.com/practc/privacy/bulletins/04-06_PDSLBurke.pdf. Accessed at: 1/10/2008.
(14) Business and professions code sections 22575-22579. Available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579. Accessed at: 30/9/2008.
(15) Center for Democracy Technology. (2007). Search Privacy Practices: A Work In Progress. Available at: http://www.cdt.org/privacy/20070808searchprivacy.pdf. Accessed at: 17/10/2008.
(16) Cooley, Alert. (2004). California Online Privacy Protection Act of 2003.- Available at: http://www.cooley.com/files/tbl_s24News%5CPDFUpload152%5C927%5CALERT-Cal_OPPA.pdf. Accessed at: 30/9/2008.
(17) Dan, Costa. (2007). You Are What You Search.- PC Magazine, vol. 26 (18).- p. 54.

(18) Duberman, Josh and Beaudet, Michael. (2000). Privacy perspectives for online searchers: Confidentiality with confidence?.- Searcher, vol. 8 (7).- pp. 32-48.
(19) Eckersley, Peter …[et al]. (2006). Six Tips to Protect Your Search Privacy.- available at: http://www.eff.org/wp/six-tips-protect-your-search-privacy. Accessed at: 20/11/2008.
(20) Edwards, Jim. (2007). Google, DoubleClick Throw Punches in Privacy War.- Adweek. vol. 48 (27).- p. 8
(21) Eecke, Patrick Van and Truyens, Maarten (2008). Recent Events in EU Internet Law.- Journal of Internet Law. vol. 11(12).- pp. 32-34.
(22) Electronic Frontier Foundation. (2008). Best practices for Online service providers.- available at: http://www.eff.org/wp/osp. Accessed at: 20/11/2008.
(23) Erickson, Markham C. and Bankston, Kevin. (2006). Should Web search data be stored?.- available at: http://online.wsj.com/public/article/SB115530662685133335-OJwdGqVy4BFV8l10JmjhOxqaoHc_20060913.html?mod=tff_main_tff_top. Accessed at: 2/10/2008.
(24) EU Panel: Delete Search Info Sooner. (2008).- The Information Management Journal, vol. 42 (4).- p. 20.
(25) EuroPriSe. (2008). First European Privacy Seal Awarded.- Available at: http://www.european-privacy-seal.eu/press-room/press-releases/20080714-europrise-press-release-en.pdf. Accessed at: 19/12/2008.
(26) Fallows, Deborah. (2005). Search Engine Users.- Available at: http://www.pewinternet.org/pdfs/PIP_Searchengine_users.pdf. Accessed at: 5/10/2008.
(27) Foley, Jayni. (2007). Are Google searches private? An originalist interpretation of the fourth amendment online communication cases.- Berkeley Technology Law Journal. vol. 22 (1).- pp. 447-475.
(28) Go Trusted.com. (2008). Surfing Anonymously. Available at: http://www.gotrusted.com/surf_anonymously.php?gclid=CNLa9ceGqpgCFQFhQgodyiY9mw. Accessed at:11/12/2008.
(29) Google Reduces Data Retention Period. (2007).- Information Management Journal, vol. 41 (5).- p22.
(30) Google. (2008 a). Privacy FAQ and Glossary. Available at: http://www.google.com/intl/en/privacy_faq.html#personalinfo. Accessed at: 1/10/2008.
(31) Google. (2008 b). Privacy Policy.- Available at: http://www.google.com/intl/en/privacypolicy.html. Accessed at: 1/10/2008.
(32) Google. (2008 c). Web History.- Available at: https://www.google.com/accounts/ServiceLogin?hl=en&continue=http://www.google.com/searchhistory/login&nui=1&service=hist. Accessed at: 16/12/2008.
(33) Ham, Shane. Should all types of data be treated equally?.- Available at: http://www.netcaucus.org/books/privacy2000/Part3.pdf. Accessed at: 14/10/2008.
(34) Hillyard, Daniel and Gauen, Mark. (2007). Issues Around the Protection or Revelation of Personal Information.- Know Techn Pol, 20.- pp.121–124.
(35) Hinman, Lawrence M. (2005). Esse est indicato in Google: Ethical and Political Issues in Search Engines.- International Review of Information Ethics, vol. 3.- pp 19-25
(36) http://myipinfo.net/
(37) Ixquick. (2008). Ixquick Q&A. Available at: http://us2.ixquick.com/eng/press/qa.pdf. Accessed at: 2/12/2008.
(38) K.Soft. G-Zapper helps you stay anonymous while searching Google. Available at: http://dummysoftware.com/gzapper.html. Accessed at: 25/10/2008.

(39) McCullagh, Declan. (2006). FAQ: Protecting yourself from search engines. Available at: http://news.cnet.com/FAQ-Protecting-yourself-from-search-engines/2100-1025_3-6103486.html. Accessed at: 22/11/2008.
(40) McCullagh, Declan and Mills, Elinor. (2006). Verbatim: Search firms surveyed on privacy. Available at: http://news.cnet.com/2100-1029_3-6202068.html. Accessed at: 25/10/2008
(41) McCullagh, Declan and Mills, Elinor. (2007). How search engines rate on privacy. Available at: http://news.cnet.com/2100-1029_3-6202068.html. Accessed at: 25/10/2008.
(42) Microsoft. (2008). Microsoft Online Privacy Statement. Available at: http://privacy.microsoft.com/en-us/fullnotice.mspx. Accessed at: 1/10/2008.
(43) Oppenheim, Charles and Natalie Pollecutt. (2000). Professional associations and ethical issues in LIS.- Journal of Librarianship and Information Science, vol 32 (4).- pp. 187-203
(44) Privacy Finder. FAQ.- Available at: http://www.privacyfinder.org/?faq=1. Accessed at: 9/12/2008.
(45) Privacy International. (2007). A Race to the Bottom - Privacy Ranking of Internet Service Companies.- Available at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961. Accessed at: 30/10/2008.
(46) Raysman, Richard and Brown, Peter. (2007). Search Engine Privacy and Data Retention.- New York Law Journal, vol. 237 (48). Available at: http://www.thelenreid.com/resources/documents/ComputerLaw_SearchEnginePrivacy_NYLJ031307.pdf. Accessed at: 2/10/2008.
(47) Resolution on Privacy Protection and Search Engines. (2006). Available at: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_annex_16_05_07_en.pdf. Accessed at: 2/9/2008.
(48) Tor. (2008 A). Abuse FAQ. Available at: https://www.torproject.org/faq-abuse.html. Accessed at:10/12/2008.
(49) Tor. (2008 B). Tor: anonymity online. Available at: http://www.torproject.org/. Accessed at:10/12/2008.
(50) Usable Privacy and Security Laboratory. Privacy Policy. Available at: http://cups.cs.cmu.edu/privacy.html. Accessed at: 10/12/2008.
(51) W3C. (2006). The Platform for Privacy Preferences 1.1 (P3P1.1) Specification.- Available at: http://www.w3.org/TR/P3P11/ . Accessed at: 25/11/2008.
(52) W3C. (2007). Platform for Privacy Preferences (P3P) Project. Available at: http://www.w3.org:80/P3P/. Accessed at: 12/12/2008.
(53) World Privacy Forum. (2006). AOL Releases The Unfiltered Search Histories Of 657,000-Plus Users; World Privacy Forum Filing FTC Complaint. Available at: www.worldprivacyforum.org. Accessed at: 25/9/2008.
(54) Yahoo. (2008 a). Ad Serving.- Available at: http://info.yahoo.com/privacy/us/yahoo/adserving/. Accessed at: 24/11/2008.
(55) Yahoo. (2008 b). Data Storage.- Available at: http://info.yahoo.com/privacy/us/yahoo/datastorage/details.html. Accessed at: 2/10/2008.
(56) Yahoo. (2008 c). web beacon.- Available at: http://info.yahoo.com/privacy/us/yahoo/webbeacons/. Accessed at: 15/10/2008.

---

(57) Yahoo. (2008 d). Yahoo! Cookies.- Available at: http://info.yahoo.com/privacy/us/yahoo/cookies/. Accessed at: 2/10/2008.

(58) Yahoo. (2008 e). Yahoo! privacy.- Available at: http://info.yahoo.com/privacy/us/yahoo/details.html. Accessed at: 2/10/2008.