IRIE
International Review of Information Ethics
ISSN 1614-1687

Vol. 17 (07/2012)

Ethics of Secrecy

edited by Daniel Nagel, Matthias Rath and Michael Zimmer

Editors of this issue:

Daniel Nagel

Attorney, BRP Renaud & Partner, Stuttgart, Germany

Prof. Dr. Matthias Rath

Director, Research Center Youth - Media – Education and Research Group Media Ethics
University of Education, Ludwigsburg, Germany

Dr. Michael Zimmer:

Director, Center for Information Policy Research
School of Information Studies, University of Wisconsin-Milwaukee, Milwaukee, USA

Editors of IRIE

Vol. 17 (07/2012)

Content

  ISSN 1614-1687

Editorial: On IRIE Vol. 17

Do you have secrets? We do! We couldn't edit this journal without! Without the anonymous peer reviewing process e.g. or the well kept secrets of our finding the subject, the guest editors etc.. This way we can do our job efficiently and you can consume the outcome – efficiently.

Try to think of it the other way round: what if everything would be fully transparent, democratic and participatory. You would be involved in a complex, very interactive process that takes its time and demands costly commitment. You would have all the information but also all the obligations associated with them. Are you – as a reader – willing to invest this effort or do you – for convenience reasons e.g. – accept this informative asymmetry. Informative asymmetries, that is what secrets finally are. And in many cases they are vital for the everyday functioning of so many procedures within our society. There are laws that protect these asymmetries because otherwise companies would go bankrupt, customers would be charged suboptimal prices and markets would collapse. Breaking these asymmetries and taking advantage of that is called insider trading, industrial espionage etc. and prosecuted by law.

On the other hand informative asymmetries are what originally markets are designed for to avoid. In a perfect market informed customers take informed decisions thus forcing companies to offer optimal prices (at least better prices than their competitors) for thus fully comparable offerings. Markets are designed to establish informative symmetries by maintaining and protecting informative asymmetries as stated above.

But not only economic structures are at stake. Take something more personal: the person itself – the meaning of the original latin notion 'persona' is 'mask'. It hides the face of the actor from the audience and is thus constitutive for the play. It hides the actor and presents the figure. Is this informative asymmetry associated with the notion 'persona' also constitutive for our being a 'person' – to keep some things hidden from others and present something defined to them? Rather to be a secret than to have secrets?

This special issue will explore the complex nature of "secrecy" in our contemporary information society. The ethical exploration of secrecy must be renewed in the face of the multiple and shifting social, political and cultural contexts in which information flows. And maybe this issue thus reduces some informative asymmetries only made possible by maintaining others as stated above.

We do thank the editors and authors of this issue for their admirable efforts to clarify the subject and questions concerned and look forward to your valuable feedback.

Sincerely yours,

The editors.

ISSN 1614-1687

Daniel Nagel, Matthias Rath, Michael Zimmer:

Secrets About Secrecy: An Introduction

The concept of "secrecy" is bound up in a variety of aspects of information ethics, sometimes in conflicting ways: respecting personal privacy and opposing undue surveillance ensures a certain level of secrecy in one's personal life and activities; the rapid development of ICTs, in particular both security technologies and surveillance mechanisms, boosted the implementation of new security measures but also heavily inflated the challenges combined therewith.

Notwithstanding the potential benefits of such systems, it has to be taken into account that the latter leave much room for challenges: traditional safeguards of secrecy are rendered obsolete and the traditional understanding of concealment is deprived of its buttress as function and even mission creep are facilitated. If information can be gathered more easily, there is no guarantee that it is only used for justified and accepted purposes and not stored, transmitted or even sold, thus, setting up a huge data-warehouses full of information that easily dwarf the Google Street View picture-collection to the significance of a small downtown public library. Moreover, sophisticated information gathering is no longer reserved to cost-intensive intelligence agencies, nor does such collection still only scratch the surface of information that is considered private or secret; it goes far beyond that. It also includes the collection of other types of information, such as e.g. biometric data, which adds a new dimension to databases and the quest to find a balanced way to address the concealment and revelation of data.

On the other hand, secrecy is often also seen as an antagonist to transparency and equality. To ensure security and public safety, government secrecy may often be justifiable; open records laws and whistleblower protections are meant to limit government secrecy and promote transparency; corporate trade secrets remain secret to protect investments and economic growth; Still – as Wikileaks prominently showed – there is a shift in public understanding of the issue on what should be kept secret, by whom and from whom. Transparency, neutrality and equal – or even universal - access to information became buzzwords of the information age. This is all the more true as the secrecy of our personal lives is increasingly shattered – and commodified – through social media.

Does the concept of secrecy need to be redefined? Is it an outdated concept of deliberate shortage of information, a last bastion of concealment against transparency and neutrality or rather a fluid context-related process within the daily interplay of individuals and organizations in a shared world?

This special issue ventures to explore the ethics of secrecy from different perspectives, frameworks, and cultures. It ranges from a basic consideration of the concept against the backdrop of Simmel's works over an elaboration of the relationship between secrecy, language and memory as well as challenges and changes of self-presentation and automated decision making within information society, to a deeper exploration of current issues and ideas such as dealing with Wikileaks and the right to be forgotten.

ISSN 1614-1687

Rafael Capurro – Raquel Capurro

Secreto, lenguaje y memoria en la sociedad de la información

Abstract:

This dialogue between a psychoanalyst (Raquel Capurro) and a specialist in information ethics (Rafael Capurro) deals with the relationship between secrecy, language and memory in the information society. The first part addresses the present debate on privacy and the Internet from a psychoanalytic perspective (Freud, Lacan), taking into consideration the relationship between language and memory. The second part deals with the concept of secrecy with regard to oblivion and censorship in the context of the digital network as a space in which seemingly anyone can tell anything to everybody. The question of "what cannot be said" is posed from a psychoanalytic perspective. The third part explores the relationship between memory and secrecy. Secrecy is defined as a "dispositif of exclusion." The concept of "information society" is contrasted to a "society of secrecy". This strategy opens a debate about the question of secrecy in the information society that might also help to disambiguate this concept when applied to concrete situations and spheres in which the question of where to draw the line arises.

Agenda:

Authors:

Prof. (em.) Dr. Rafael Capurro:

- Redtenbacherstrasse 9, 76133 Karlsruhe, Germany
- ☎ + 49 - 721 - 98 22 9 22 , ✉ rafael@capurro.de, 💻 www.capurro.de
- Relevant publications:
  - Rafael Capurro - John Holgate (eds.). Messages and Messengers. Angeletics as an Approach to the Phenomenology of Communication. Munich: Fink 2011.
  - Intercultural Information Ethics. In: Kenneth Einar Himma and Herman T. Tavani (eds.): The Handbook of Information and Computer Ethics. New Jersey: Wiley 2008, p. 639-665.

Psyc. Raquel Capurro:

- Benito Blanco 747, Ap. 701, 11300 Montevideo, Uruguay.
- ☎ + 598 – 2 - 7106129 , ✉ recap@internet.com.uy
- Relevant publications:
  - Comte. Actualidad de una herencia. Mexico: Epeele 1999. (Trad. al francés: Le positivisme est un culte des morts. Paris: Epel 2001).
  - El sexo y su sombra. Del misterioso hermafrodita de Michel Foucault, México: Epeele 2004.

ISSN 1614-1687

1 Introducción

Rafael Creo que existe hoy un "malestar en la cultura"[1], con relación a la comunicación digital. Se percibe tanto una euforia en Internet con relación a la posibilidad de *decir todo a todos*, sin límites de espacio y tiempo pero sobre todo de contenido. También se da una inseguridad provocada a nivel del *e-mail* diario por el SPAM y los virus debido a la influencia cada día mayor de la red digital en todos los aspectos de la vida social.

Vivimos en una *sociedad de mensajes digitales* en la que parece haberse realizado aquel sueño de la Ilustración de eliminar todo tipo de barreras o de *censura* impuestas por el poder político y su aliados, el poder militar, religioso y moral. ¿Quién puede enviar mensajes? ¿de qué tipo? ¿a quién? ¿en qué medio? ¿con qué alcance espacio-temporal? ¿con qué posibilidad de que puedan ser o no distorsionadas? ¿con qué formas de ser conservadas? Y, sobre todo, ¿cómo sustraerlas al alcance de quienes no debieran conocerlas sin previo consentimiento de los sujetos que los producen y sustentan? ¿Y todo esto en base a qué regla o programa y con qué repercusiones a nivel individual y social? En una palabra: ¿cuál es el lugar del secreto, en un sentido amplio de este concepto, en la sociedad de la información digital?

Es una situación paradójica si la contrastamos con el siglo XIX y comienzos del siglo XX, es decir con la época de Freud como la describe, por ejemplo, en el capítulo 3 de su ensayo sobre el "malestar en la cultura" publicado en 1930[2]. Paradójicamente la ciencia y la técnica, el meollo de la cultura, que consideró como "sublimación" ("Sublimierung") de los instintos se ha vuelto un problema. ¿Cómo ves tú estos conflictos y en especial cómo ves tú el fenómeno de la delimitación entre lo público y lo secreto así como entre lo público y lo privado? Naturalmente que el tema del secreto va mas allá de la discusión sobre la privacidad tan virulenta hoy en día. El secreto está conectado al fenómeno de la memoria, individual y colectiva: sólo podemos guardar un secreto si de alguna manera lo fijamos en la memoria para lo cual necesitamos el lenguaje, y, en la sociedad de la información actual, a la memoria digital.

Raquel. Empezar un diálogo sobre ese tema, me parece interesante. El asunto tiene muchas puntas, por ejemplo, como tú señalas, el de la formulación de diferencias entre lo público y lo privado. Las diferencias hoy aparecen multiplicadas y quizá sea más acertado hablar de *los* públicos adecuados a cada tipo de comunicación. Si consideramos además la dimensión política de estos temas relativos a la información y al secreto, hemos vivido en los últimos años, en Uruguay, las tensiones sociales derivadas de políticas en donde los archivos secretos de las dictaduras militares, el secreto "militar", han jugado claramente como factor de poder. Siguiendo a Michel Foucault, no creo que lo que puede saberse y decirse en una sociedad, esté por fuera de esa lucha de poderes que constituyen a la vida social. Los secretos industriales ponen en evidencia el capital que representan ciertos conocimientos en las luchas competitivas por el mercado. Ya sea como secreto o como censura, el circuito de las palabras ve marcados sus límites epocales.

Pero quiero llevar mi intervención a un campo más restringido, el campo del psicoanálisis, en donde se pone en juego un dispositivo que pareciera otorgar todas las libertades al decir y al recordar de un individuo. Espacio de privacidad en donde se hará público ante el analista y para quien habla aquello que allí será dicho. ¿Qué sucede cuando la única regla de juego es decirle al analizante "Diga sus ocurrencias"? ¿Qué sucede en esa experiencia? Freud fue sorprendido por la conexión que se establecía entre ciertos recuerdos que afloraban y los síntomas que aquejaban a sus pacientes. Esta cuestión no tiene hoy indudablemente el mismo marco de referencia que tuvo Freud. Se hace patente, creo, en tu misma intervención de apertura de este diálogo. Estamos lejos de las teorizaciones de Freud. Sí, pero también estamos lejos de prácticas del lenguaje que, como el psicoanálisis, solo pueden sostenerse en otra concepción de la relación entre el

[1] Freud 1974.

[2] Freud op.cit.

ISSN 1614-1687

sujeto y la lengua que habita y lo habita. No veo como abordar los problemas de la memoria y del secreto en el psicoanálisis sin señalar este punto de partida. La regla analítica de la asociación libre puede guiar una cura en la medida en que el yo acepta soltar sus riendas y deja vagabundear sus pensamientos. En medio de esa situación emergen recuerdos evocados con ciertas palabras, y no otras, con el sabor, el timbre y el saber de la lengua particular del hablante que allí está. Esos recuerdos, que Freud llamó encubridores, permiten tramitar los entramados libidinales que viajan en las palabras, en sus silencios, en los síntomas que, con su críptico cifrado, señalan vivamente el fracaso de las fuerzas opuestas a la traducción en palabras de las vivencias subjetivas. Freud llamó a esta fuerza operativa y silenciadora, "Verdrängung" y creyó hasta 1914 que bastaba el dispositivo de la asociación libre para que finalmente la rememoración de lo traumático aflorara en el decir. Y bien, no. "Wiederholung": aquello que no se recuerda retorna, pero no como recuerdo, sino en los actos que transferencialmente ligan analizante y analista. De ahí un atolladero freudiano. ¿Cómo tratarlo?

En el plano social esta pregunta se instaló de otra manera durante el correr del siglo XX. El espanto de los genocidios cometidos, de los actos de barbarie, que afrentaron y afrentan la convivencia, se levantó la consigna de la memoria contra la repetición. Los pueblos que no recuerdan su historia están condenados a repetirla, se ha dicho, y hasta cierto punto podemos acordarlo. Pero… ¿acaso la memoria tiene operatividad respecto a la repetición? Esto requiere un ensanchamiento de la problemática de abordaje. En la década del 50 varias disciplinas, entre ellas el psicoanálisis, pudieron plantearse la relación del sujeto al lenguaje en el nuevo marco de la lingüística saussuriana. Fue un primer tiempo en el que Jacques Lacan buscó respuesta a esa pregunta freudiana releyendo *La Carta robada* de Edgar A. Poe. ¿La repetición es acaso la simple reproducción de una conducta regida por el retorno de un significante reprimido? Fue la primera posición de Lacan que leemos por ejemplo en 1955: "Nuestra investigación nos ha llevado al punto de reconocer que el automatismo de repetición ("Wiederholungszwang") toma su principio de lo que hemos llamado la insistencia de la cadena significante".[3]

Sin embargo, los agregados que Lacan fue haciendo a ese texto permiten leer un cambio en su posición. Como lo señala unos años después, lo que está en juego aquí, a lo que hay que dar respuesta "es a la estructura misma de la determinación" del hablante.[4] Lacan se deja guiar por el ternario que ya propuso en 1953 y que rige su producción teórica: el hablante existe en el imaginario, simbólico y real, registros de sus experiencias, registros – dirá en la década del 70 – que se anudan en cadenas borromeas.

2 Lenguaje, memoria y red digital

Rafael Si me permites hacer de nuevo el pasaje de lo individual a lo social: un efecto del psicoanálisis freudiano podría concebirse como el deseo de "otorgar todas las libertades al decir y al recordar", como tú dices, en base a un nuevo medio.

Los orígenes de la red digital que llamamos internet se encuentran en una necesidad social de comunicar todo a todos como la piensan los filósofos de la ilustración con su crítica a la censura concibiendo la utopía de una sociedad con una memoria abierta y accesible a todos, en la cual todos puedan decir todo y recordar todo. Esto se traduce luego, por ejemplo, en las libertades de la generación de 1968 como reacción a la contrautopía del fascismo donde nadie podía decir nada a nadie sin tener en cuenta que eso era un peligro mortal. El fascismo concibe la 'sociedad del secreto' desde arriba, con una jerarquía de poder basada en archivos y mensajes administrados por una policía secreta, la *Gestapo* (abreviación de "Geheime Staatspolizei" o policía secreta del estado). Pero también los fascismos de izquierda, el stalinismo por ejemplo, basan su poder en este esquema y liquidan a millones.

[3] Lacan 1966, p. 11.

[4] Ibid. p. 52

No es entonces por casualidad que una máquina que obedece órdenes ciegamente como es la computadora, se transforme paradójicamente en un medio social en el cual se proyecta un ideal de información generalizada, una 'sociedad de la información' como contra-dicción a una 'sociedad del secreto'. Visto así, secreto e información son conceptos opuestos. Pero esta oposición es relativa, ya que hay informaciones en la sociedad de la información digital que quedan restringidas a un grupo. Todo secreto tiene una dimensión social. Nadie puede tener algo secreto concebido desde y para sí mismo.

Hablar de secreto e información es por tanto, como tú lo indicas, hablar de y desde el lenguaje como el horizonte en el que forman y transforman los diversos modelos individuales y sociales de memoria e información. Aquí entra el sustento de los significantes como preludio a lo que en la técnica de la red digital es el sustento de un traductor que permite que las distintas computadoras puedan intercambiar mensajes a pesar de hablar lenguajes diferentes.

Lo que acontece cuando estamos en la red de los cuerpos digitales que llamamos internet es, por un lado, un proceso 'maquinal' o subsemántico entrecruzado con el lenguaje humano. Desde el punto de vista semántico, la red digital es una máquina gigantesca de repetición donde todo está en espera que alguien piense que lo que está ahí expuesto sea visto como algo relevante es decir como un mensaje en espera de un asentimiento. El sujeto que es así tocado por la información queda sujetado a ella cuando esta se vuelve mensaje y el usuario se vuelve su cómplice.

Por cierto que en este complejo sistema de traducciones todo queda abierto a 'traiciones' puesto que lo que es expresado en un lenguaje sólo puede ser referido en el otro con un código diverso. Pero siendo así como ambos sistemas son sistemas del sujeto, hay siempre algo que les es común. Lo que le duele al sujeto y es censurado queda enganchando en diversos códigos, con distintos sistemas de secreto y memoria. En el plano social los sistemas criptográficos son un intento ensamblador de traducir significados informacionales en significantes secretos. Visto así podríamos definir el fenómeno del secreto como el pasaje de un significado expresado en un lenguaje a un lenguaje de otro género utilizando para ello un traductor. La red digital ofrece por un lado la posibilidad de poner a disposición de forma infinita todos los significados posibles, pero lo hace sirviéndose de un significante que es parte de otro género, la computadora. Esto hace posible desde el inicio mismo de la sociedad de la información la creación de una memoria accesible solamente a quienes puedan comprender su lenguaje secreto. Creo que esto no es propio de la sociedad de la información actual, sino que caracteriza a toda sociedad humana en tanto en cuanto su habla es desde su propio origen biológico un lenguaje mixto, al que los hablantes están sujetos en el momento mismo en que se conciben como sujetos hablantes y capaces de informar pero también de guardar un secreto.

Raquel Has llevado el tema a aspectos muy interesantes que me plantean el problema de si no le estarías dando una compatibilidad demasiado extensa a lo que sucede en distintos registros que tu llamas "de lenguaje". Esto nos lleva a prestar particular atención a este su modo de jugar con la polifonía de los sonidos con los que cifra el real y lo convierte, al decirlo, en acontecimiento y/o recuerdo, pero también en fijación virtualmente móvil. Cuando la fijación queda rígida, y constituye un signo, como aquellos cifrados en mensajes codificados, de máquinas, (como en el semáforo) o de animales (condicionamientos conductuales) y/o de estructuras celulares o genéticas estamos en un sector de preguntas que son diferentes a las que se plantean si no olvidamos la poética del lenguaje. Esta aparece a veces como irrupción loca cuando alguien por ejemplo, le atribuye sentidos incompartibles a los cambios de luces de un semáforo. Ya sea con fines científicos, bélicos – o, a nivel individual, sintomáticos – estamos ante una situación peculiar que plantea su descifrado y su integración o no, al fluir polivalente del decir. Por eso me parece que el concepto mismo de traducción ha de ser considerado más de cerca ya que tal como tu lo usas implica operaciones diversas: de cifrado, de descifrado, pasaje de sistemas de escritura a otros, transcripciones de sonido y por último, pasajes de sentido de una lengua a otra, a lo que propiamente se ha llamado traducción. La rememoración juega con todas estas posibilidades, como lo da a leer la obra de Proust, por ejemplo. Las fallas en el sistema neuronal traen consecuencias para el hablante, pero hay allí una discontinuidad a señalar, así como hay una discontinuidad, un hiato entre lo que ocurre y las versiones que se fabrican sobre ello. Lacan, en 1964, señalaba que no toda la vida pulsional nos es asequible a nosotros

mismos, sólo aquello que de la sexualidad pasa "por los desfiladeros del significante". En esa línea la experiencia analítica indica que "todo" no puede decirse y que ese límite es distinto al de la censura o el secreto, pues es un límite de nuestra con-formación misma. Por eso concuerdo en que "una necesidad social de comunicar todo a todos" como la piensan los filósofos de la ilustración con su crítica a la censura sitúa la utopía de una sociedad con una memoria abierta y accesible a todos, en la cual todos puedan decir todo y recordar todo.

De modo más amplio en este nivel se plantea el problema mismo del historiador así como el del testigo. En estos días me encontré con la creación en Uruguay de un "museo de la memoria" que, como sucede con muchos otros creados en el mundo, busca preservar del olvido acontecimientos que han sido traumáticos para una generación. ¿Cómo se sitúa la nueva generación ante aquello que recibe a modo de legado? Toda una cuestión.

3 Olvido, censura y secreto

Rafael Con respecto a lo que indicas al final sobre el "decir verdadero" como lo plantea Michel Foucault en su curso sobre la *parrhesía* [5], creo que es importante ver este tema tomando como contraste la tradición oriental, y en especial la de la China clásica, del "decir indirecto" como lo investiga François Julien haciendo especial referencia al sabio taoista Dshuang Dsi (365-290 AC).[6] En otra ocasión he tratado de mostrar la relevancia de esta contraposición entre "decir directo" y "decir indirecto" para la configuración de distintos tipos de sociedades de la información.[7] Lo que dice Lacan sobre la relación entre la mano y el agua del río expresa la relación taoista con la naturaleza como un proceso ("dao") en el que estamos inmersos y que "alimenta la vida" como dice Jullien.[8]

Como tú dices, es importante hacer una diferencia entre lo que no se puede decir y permanece secreto pero que va pasando por los diversos significantes o en la manera del "decir indirecto" y el concepto de secreto asociado a la censura. Además está también el concepto de privacidad tanto en el sentido de poder disponer libremente de lo que quiero decir a otros como el de impedir a que otros entren en el espacio privado. Cuando los filósofos de la ilustración hablan de libertad de censura y en el siglo XIX de libertad de prensa se refieren, como tú dices, al concepto de secreto como algo impuesto por un poder que me obliga a no poder comunicar algo que querría que otros supieran. La necesidad social de poder comunicar todo a todos surge como utopía informacional en este contexto. Pero al mismo tiempo hay límites de este deseo social que se manifiestan por ejemplo en la necesidad de mantener secretos diversos tipos de conocimientos como los llamados secretos de estado o también los secretos de una empresa que protege su saber frente a la posibilidad de que sus productos sean copiados por los competidores.

En estos y otros casos ubicamos el concepto de secreto en el ámbito de poder el cual también pone límites (variables) a la utopía del poder comunicar todo a todos. Creo que estos límites no son sólo un problema de censura sino también que están dados por el carácter esencialmente limitado de la comunicación humana. Por otro lado el desarrollo actual de la red muestra la inmensa atracción de esa máxima ética: '¡Comunica todo a todos!' que se transforma en un imperativo moral y conduce al desarrollo de los movimientos sociales en la red discutidos hoy bajo el término de Web 2.0. Dichos movimientos que comenzaron con listas de mensajes y *chats* se transforman ahora en grupos de todo tipo en el que los integrantes se reúnen en torno a un interés común, intercambiando todo tipo de mensajes multimediales en torno a un *blog*, construyendo un *wiki*, o intercambiando videos en *YouTube*. Esto se expresa también en el campo de movimientos

[5] Foucault 1983.

[6] Jullien 1995.

[7] Capurro 2006.

[8] Jullien 2005.

políticos de todo tipo y color asi como grupos al margen o en contra de la legalidad como son por ejemplo los de pornografía infantil.

Creo que tendríamos que profundizar la relación entre secreto y memoria tomando como hilo conductor los tres sentidos de secreto que vamos elaborando, es decir:

1) secreto como dimensión de lo decible sólo indirectamente,

2) secreto como lo reprimido por procesos de censura y

3) secreto como lo que pertenece al campo privado.

Esta diferenciación tiene tal vez la desventaja de ensanchar demasiado el contenido intencional del concepto de secreto, sobre todo en el caso de la tercera definición que tiene relación con lo íntimo y confidencial.

El conservar un secreto ("Geheimhaltung") es, como lo indica Hemma Boneberg,[9] una estrategia de la evolución en el sentido de una máscara o un camuflaje que impide que los competidores en el campo de la alimentación o la reproducción puedan sacar provecho del otro. En el humano se produce un proceso de segundo grado para conservar un secreto en base a signos que representan lo ausente en lo presente, haciéndolo al mismo tiempo patente. En otras palabras un signo secreto patente está codificado en forma doble.

Estamos en el campo del saber y del querer callarse en determinadas situaciones. Lo cual nos lleva una vez más a las pregunta de ¿quién dice o no qué cosa a quién, en qué situación, con qué razones etc.? Podríamos discutir la tesis que secreto y memoria, vistos en esta perspectiva amplia semántica e histórica, son algo específicamente humano en tanto que en ellos se juega un proceso de velamiento y develamiento de segundo grado, es decir codificado y reflexionado linguísticamente. Para el filósofo Georg Simmel la forma negativa específica de desocultamiento de un secreto es la traición ("Verrat").[10]

Raquel Retomo algunas de tus incursiones: "es importante – dices – hacer una diferencia entre lo que no se puede decir y permanece secreto pero que va pasando por los diversos significantes o en la manera del "decir indirecto" y el concepto de secreto asociado a la censura". Sí, acuerdo contigo y agrego una complejidad más: lo que permanece secreto es algo que se supone inscripto en algún sistema de escritura o codificación. Esto es a diferencia de aquello que se experimenta y no tiene inscripción. Hay experiencias centrales que no pueden decirse, y no por ser secretas ni por estar reprimidas, sino porque no hay manera de inscribirlas: supongo que a ello alude Wittgenstein al final del "Tractatus".[11] Quedar mudos ante la muerte no es quedar con un secreto, ni ante algo reprimido sino ante la imposibilidad de decir. Todo lo que allí se diga no anulará ese vacío, el decir indirecto le hará borde ¿? pero no creo que pueda llamarse a eso que no se puede decir un secreto, salvo en forma metafórica. Creo que estamos, como decía Wittgenstein, dándonos de cabeza contra los muros del lenguaje. Esto da el marco del decir. Su límite.

Rescato contigo el valor del decir indirecto y recordé a propósito el libro de Leo Strauss sobre "La persecución y el arte de escribir", en el que analiza los procedimientos alusivos de Maimónides para hacerse entender por quienes quería hacerse entender y quedar opaco para los demás.[12] Quienes hemos vivido

[9] Boneberg 1999.

[10] Simmel 1995, p. 409.

[11] Wittgenstein 1984.

[12] Strauss 1989.

situaciones de persecución política sabemos que la alusión se vuelve en esas circunstancias un refinado método de astucias para hacer llegar un mensaje a ciertos destinatarios y no a otros.

El darle la palabra a un analizante, supone darle un lugar a una verdad que está ahí, sin que sepamos qué dice como algo "casi-inolvidable" [13] para que al fin pueda descansar en paz. El mensaje críptico a leer en sueños y síntomas no debiera instalarse como un imperativo de recordar ni de abolir el secreto, lo que sólo serían nuevas imposiciones superyoicas: "Hay que decirlo todo, recordarlo y confesarlo todo". Si así ubica el analista la regla de juego, bien merece las críticas de Foucault cuando observa la puesta en funcionamiento en el siglo XIX del dispositivo de la sexualidad como dispositivo de confesión y cuando considera que el psicoanálisis sería su última producción. Pero si como psicoanalista hago mía la crítica foucaultiana, diré que se trata en la experiencia del análisis de esos juegos de verdad que el mismo Foucault señala y en parte toma de Wittgenstein. Esos juegos en el análisis tienen reglas, que no son de revelar lo secreto ni de ser sinceros, sino de decir las ocurrencias del momento. Ese juego, señala Jean Allouch,[14] abre también la puerta al engaño, a la imaginación, a los recuerdos, etc.

Creo que recortamos así una pregunta acerca del estatuto del secreto, ya sea individual, familiar, político, militar, industrial, etc. Hay archivos secretos. Aquellos a los que no se llega fácil.[15] También los archivos se depositan allí donde la memoria falla. Estos no exigen el secreto. Lo secreto es activamente puesto aparte por alguien. Es un dispositivo de exclusión. Cuando alguien habla y se le hace presente un secreto que no quiere decir, lo que ocurre a menudo es que enmudece, pues todo su flujo asociativo queda enlazado a ese secreto. Por eso en un análisis el secreto trampea la regla de juego. "Diga lo que se le ocurra".

Ahora y con estos rodeos llego a tu propuesta: "Creo que tendríamos que profundizar la relación entre secreto y memoria tomando como hilo conductor los tres sentidos de secreto que vamos elaborando, es decir:

1) secreto como dimensión de lo decible sólo indirectamente,

2) secreto como lo reprimido por procesos de censura y

3) secreto como lo que pertenece al campo privado."

Esta diferenciación tiene tal vez la desventaja de ensanchar demasiado el contenido intencional del concepto de secreto, sobre todo en el caso de la tercera definición que tiene relación con lo íntimo y confidencial. Y llego a la conclusión que está 1. el decir indirecto; 2. el retorno de lo reprimido 3. y el secreto que se instaura en la esfera pública o privada. Como verás me inclino a no seguirte en esa ampliación del concepto de secreto. Quisiera detenerme por último en la censura tal como se instaura en la esfera pública, por ejemplo, la censura de lo que se escribe. La censura aparece como un movimiento de tachadura que deja ver aunque más no sea por los blancos que instaura en los periódicos como señalaba Freud, una operación en la que algo es puesto afuera. Freud no identifica censura y represión.

Respecto al meollo del asunto quiero enfatizar desde el punto de vista en que estoy colocada

1. la riqueza y complejidad de las relaciones del hablante con la lengua que lo habita y el riesgo de reducir esa complejidad.

[13] Allouch 1998.

[14] Allouch, op.cit.

[15] Derrida 1995.

2. Una forma de incurrir en ese riesgo sería alimentar la utopía de que todo puede decirse en la red, y en los encuentros virtuales. Rescatar pues el decir de los cuerpos vivos y presentes que disponen también de esta vía para entrar en comunicación.

3. Respecto a la relación memoria secreto: creo que acentuaría su estrecha conexión con los poderes en juego, cada vez que se traman con los saberes de la época. Los historiadores están concernidos en forma particular por esta cuestión de lo que se selecciona y se silencia al hacer historia, así como cada persona cuando historiza tramos de su vida. Pero lo que se silencia no necesariamente se convierte en secreto.

4 Memoria y secreto

Rafael Concuerdo contigo en que es más correcto definir al término secreto como algo que se instaura en la interfaz de lo que en una sociedad se considera como privado y público, siendo estas categorías de segundo orden, es decir que no son propiedades de algo (un texto, una foto, un evento de cualquier tipo) sino algo que se les atribuye en un juego social. La diferencia entre lo privado y lo secreto hace relación, en el caso del secreto, a algo que se quiere activamente impedir que otros tengan noticia. En un sentido todavía más estricto podríamos añadir que la razón de mantener algo secreto es que su conocimiento por terceras partes puede ser de daño (directa o indirectamente) para quien lo custodia. Además podríamos distinguir tipos de secretos de acuerdo a su contenido y el estatuto o situación de la persona o el grupo que lo custodia, como ser por ejemplo el secreto de estado. Finalmente habría que analizar no sólo la relación entre secreto y lenguaje sino también la atribución de la característica de secreto a todo tipo de objetos y de relaciones entre los mismos. Todo un cosmos que ensancha lo que se suele llamar criptología, un término que relaciona lo oculto (*kryptós*) con el lenguaje (*lógos*) y alude a las técnicas para ocultarlo.

Te propongo hacer una distinción conceptual entre 'sociedad de la información' y 'sociedad del secreto'. Llamo 'sociedad de la información' a aquella que está estructurada con una tendencia horizontal o democrática, mientras que la 'sociedad del secreto' tiende a esquemas jerárquicos o verticales, como es el caso de sociedades fascistas del siglo pasado, la del *Ancien Régime* francés así como las sociedades medievales y las de la antigüedad con excepción (relativa) de la democracia griega y sus sucesoras, en especial las democracias modernas. En las sociedades del secreto tiende a eliminarse el dominio privado o este vale sólo para una persona, un partido, una casta... que guarda secreto su saber para el resto de la sociedad, no permitiendo que nadie tenga acceso a su poder.

Las sociedades democráticas se caracterizan por tener un dispositivo para descubrir algo (supuestamente) ilegal que alguien intenta ocultar – este es el sentido de la libertad de prensa como un cuarto poder político – y otro dispositivo, el de la protección de datos personales, que impide que el estado o grupos sociales, se sirven de informaciones ilegalmente o sin el consentimiento adecuado. A fines del siglo XX la libertad de prensa tiende a abusar de su poder no sólo como instrumento político sino también sobrepasando los límites de la privacidad en busca de escándalos que le procuren un mayor rendimiento económico. El estado, a su vez, se sirve cada vez más de la red digital mundial y de todo tipo de instrumentos de observación y control, para, en los mejores casos, aumentar la seguridad social al costo de las libertades individuales. Esta tendencia se acelera sobre todo después de los acontecimientos del 11 de setiembre de 2001 en Estados Unidos y la consecuente lucha contra el terrorismo. Pasamos entonces de la democracia basada en la libertad de prensa y la abolición de la censura, sobre todo en relación a los libros y demás productos de la era de Gutenberg, por la mediocracia del siglo XX hasta llegar a la 'netocracia' (*netocracy*), o poder de la red, de fines del siglo pasado y comienzos del siglo XXI. Lo curioso es que la pérdida del sentido de lo privado no sólo no es vista a menudo como algo negativo, sino que gran número de personas ponen libremente en la red aquello que antes se consideraba como privado y en muchos casos, sobre todo en el plano sexual, como secreto o íntimo. El exhibicionismo pasa a ser un valor social y la red digital se transforma cada vez más un medio de exhibicionismo.

Pienso que toda sociedad humana funciona con el código desvelar/ocultar[16] y que dicho código es un "concepto de la reflexión" ("Reflexionsbegriff") como los llama Kant, en contraposición a conceptos que expresan cualidades de objetos La base sobre la que descansa este código desvelar/ocultar es la memoria, tanto individual como colectiva. La cual a su vez se sirve del dispositivo del olvido y del recuerdo para frenar y reprimir o para acelerar, como catalizador, los cambios sociales y en especial las reglas morales vigentes. Vista así, la ética, como la concibe Michel Foucault en sus clases sobre la *parrhesía* citadas anteriormente, es un dispositivo catalizador o un síntoma del desacuerdo entre una interpretación fija, en el sentido de "cualidad de objeto", de lo que se ve como moralmente permitido de ser ocultado o descubierto. En muchos casos se produce un efecto social "amfibólico" (en sentido Kantiano) del cual se sirven abundamente los medios de masas en tanto que actúan como altoparlantes de la moral vigente o de lo que se considera como 'políticamente correcto'.

Los *blogs* y los *wikis* así como todo tipos de foros digitales y redes sociales de intercambio, como Facebook y Twitter, en todos los campos imaginables y abarcando tanto a grandes comunidades de millones de participantes hasta grupos selectos son índices de un cambio de las categorías de secreto y desvelamiento que cuestionan muchas delimitaciones y reglas morales y legales vigentes en comunidades, culturas y estructuras políticas así como complejos mediáticos de difusión vertical de mensajes, cuyas consecuencias positivas y negativas a distintos niveles recién empezamos a percibir y a pensar.

Raquel Casi me quedaría callada después de tu excelente desarrollo pero en el mail que me dirigías acompañando este texto pasó algo que me parece importante hacer público. Me escribes que leíste en el último número del *Magazine littéraire*[17] dedicado a "les ecritures du moi, autobiographie, journal intime, autofiction" una expresión paradójica "journal extime". Esa expresión operó como una llave, una clave olvidada. ¿Cómo no había recordado ese término central que inventa Lacan para designar el estatuto particular que cobra a veces el decir o el hacer público?

Voy a situar ese término para luego responder a esa pregunta. En su seminario sobre "La ética del psicoanálisis"[18] Lacan se encuentra hablando del arte, en particular de las anamorfosis, y alude a las pinturas rupestres de las cuevas de Altamira: esa cueva en donde sorprendentes imágenes fueron dejadas allí como pruebas objetivas del ejercicio artístico en un pasado remoto, pero pruebas subjetivas también pues a través del tiempo nosotros, al contemplarlas, somos puestos a prueba en ese encuentro. Ellas nos remiten al ejercicio de creación que se organiza en torno a un vacío, delimitado, el de una pared, el de una página en blanco, el de una pantalla. Ese lugar vacío, 'presentificado' por la caverna (de Altamira, de Platón, de nuestras pantallas) opera, según Lacan como lugar central desde donde opera la creación a la que califica como "esa exterioridad íntima, extimidad, que es la Cosa"[19] en cuya cercanía algo se produce.

La Cosa, con acentos kantianos, remite a Freud cuando en sus primeros escritos, que Lacan trabajaba en ese año, describe, en las experiencias iniciales del encuentro con el prójimo, la presencia de dos componentes, aquel que se ofrece al discernimiento y el que permanece como Cosa que escapa al sujeto, "das Ding", dice Freud. En 1969, Lacan retoma el término, "éxtimo" y precisa, "lo que nos está más próximo, siéndonos a la vez exterior" ("ce qui nous est le plus prochain tout en nous étant extérieur".[20] El espacio de la exterioridad-interioridad que la caverna abriga, la extimidad, muestra que la topología para pensar la relación del sujeto con el campo del Otro no puede recurrir ya a la simplificación de un adentro y un afuera. De ahí todas las búsquedas en esta dirección efectuadas por Lacan a partir de esos años.

[16] Simmel, op.cit., p. 405-406.

[17] Geffroy 2007.

[18] Lacan 1960

[19] Lacan 1960.

[20] Lacan 2006.

Retornando al e-mail que me enviaste: al leerlo en mi pantalla una palabra resonó y despertó lo mío que necesitaba ese recorrido éxtimo para reaparecer. Reconocerlo, en este caso era fácil, no siempre lo es, y hacer con ello algo nuevo. Este pasaje por el campo del Otro permite encontrar lo que ya no merece ser llamado "propio", pero que permite al sujeto subjetivarse allí.

5 Conclusión

Rafael Un hermoso ejemplo de memoria a través del otro y también a través de la pantalla digital y global que llamamos internet. La red digital mundial es algo así como un modo óntico del "ser-en-el-mundo" (M. Heidegger) en un medio que nos abarca pero sin ser una transcendencia metafísica.

El subjetivarse en y a través de la red en las diversas formas posibilitadas por los nuevos dispositivos de la Web 2.0 y su intersección con los móviles celulares así como con todo tipo de comunicación digital que *enreda* al cuerpo humano individual con su entorno social, político y ecológico, implica entrar en este juego de memoria y olvido digital con todas las ambigüedades, promesas, desilusiones, y peligros totalitarios que este medio hace posible siendo muchas veces difícil trazar la línea divisoria entre un estado democrático que intenta proteger a sus ciudadanos reduciendo su privacidad y opacidad en base a técnicas digitales de observación y control que pueden desembocar casi sin percibirlo en una sociedad de control.

Visto así, el tema del secreto entendido como algo que el sujeto no desea que llegue a ser de conocimiento público, se vuelve paradójicamente un asunto de capital importancia para una sociedad democrática. El derecho a la privacidad se puede entender entonces no sólo como el derecho a impedir que el estado entre en el recinto del sujeto, sino también en el sentido de que el sujeto tiene derecho a decidir cuál información que le incumbe, a distintos niveles y en relación a distintas prácticas, va a ser abierta al público con su consentimiento. En Alemania existe este derecho bajo el término de la "autodeterminación informacional" ("informationelle Selbstbestimmung").

Recordemos también que es justamente la red digital mundial la que provoca la crisis de aquellos regímenes modernos como son las patentes y el derecho de autor que fueron creados justamente para evitar los conocimientos secretos, proporcionando la protección legal a los inventores, autores y creadores artisticos. Tanto la ciencia como la economía modernas no pueden avanzar si no se comunican públicamente los conocimientos. Pero, al mismo tiempo, dicha comunicación no es ni absoluta ni está desprovista de dispositivos de seguridad con los cuales se crean diversas formas de privacidad y límites de acceso. Ninguna empresa, como tampoco el estado, pueden prescindir de plantearse la pregunta por el límite entre lo público y lo privado incluyendo lo estrictamente confidencial o secreto. Son innumerables los casos en los que se pueden observar la ambigüedad de dichas delimitaciones como, por ejemplo, el no publicar resultados negativos en el caso de una investigación científica cuyo conocimiento pueda llevar a cuestionar un proyecto o un producto, como tú lo indicabas ya al comienzo de este diálogo, así como también las innumerables formas de re-escribir el pasado de un país o de una empresa o de una persona... de tal manera que sólo se recuerde aquello que es conveniente a quienes detentan el poder.

Podemos decir entonces que la dimensión de lo secreto como límite de algo segregado, es inseparable de lo abierto o público de tal modo que el código secreto/público que se entrecruza con el de memoria/olvido es algo que caracteriza a toda sociedad humana en cuanto esta se constituye en el lenguaje. En este diálogo hemos intentado mostrar, de forma muy sintética y a menudo tangencial, cómo dichos códigos se juegan, entrecruzándose a nivel del individuo en el psicoanálisis y a nivel de la sociedad en el medio digital. Tu indicabas al comienzo la ambivalencia del medio digital que paga sus posibilidades de comunicación global al costo de un empobrecimiento de las numerosas dimensiones de la comunicación humana. Pero también podemos decir que la red digital ofrece nuevas posibilidades de interacción social casi inimaginables hace, digamos, unos cincuenta años. Estas posibilidades implican también una reinterpretación de los códigos que mencionaba recién.

Creo que podemos resumir el tema que hemos tratado constatando la ambigüedad del secreto como dispositivo de exclusión. Por un lado vemos claramente que a nivel político hay muchas veces gran interés en no develar un pasado relacionado, por ejemplo, con heridas provocadas por regímenes dictatoriales. El secreto como dispositivo de represión en la memoria social tiene en este caso un carácter de censura y bloqueo de un proceso de recuperación de una identidad lesionada o de una herida abierta que no se quiere reconocer como tal. Pero por otro lado tenemos aspectos de la vida diaria que todos pensamos que deben ser protegidos y guardados en forma secreta dado que en caso contrario se produce una situación de peligro. La constitución alemana ("*Grundgesetz*") declara al secreto postal como un derecho fundamental y también lo hace la *Declaración Universal de Derechos Humanos* en el artículo 12.

Naturalmente que hay que ver a este derecho en conjunción, por ejemplo, con la libertad de prensa. Está claro también que la protección de la correspondencia privada establece una relación de secreto frente a la inferencia del estado que no es igual, por ejemplo, a la del intento del estado de mantener secretos recuerdos sociales que puedan poner en peligro a poderes vigentes. Hay aquí una relación entre secreto y tiempo que sería importante profundizar en el marco de una antropología cultural y filosófica.

Lo que caracteriza a la problemática del secreto en la sociedad de la información digital es un *cambio topológico* del secreto como algo relacionado al individuo humano en su *concreción corporal y psíquica*, a algo relacionado con la exterioridad de su intimidad individual y/o social en *aparatos de memoria digital* como son el *laptop* y el celular. Los debates actuales sobre las posibles formas de observación e intrusión estatal secreta con la fundamentación de la seguridad pública frente a la amenaza del terrorismo son un indicio claro de este cambio topológico. En otras palabras, cuando hablamos de secreto y memoria en el contexto actual de la sociedad de la información digital abarcando desde los secretos individuales, pasando por los secretos empresariales hasta los secretos de estado, nos estamos refiriendo sobre todo a los aparatos digitales en los cuales dichos secretos están almacenados siendo protegidos por leyes fundamentales y específicas.

El debate que se abre es entonces el de determinar cuáles son los límites éticos y legales de dicha protección en circunstancias concretas, es decir, de determinar cuándo se pasa a borrar la diferencia entre lo secreto y lo público de tal manera que el espejismo de una sociedad abierta que no admita ningún tipo de protección a la privacidad – el creer que todos pueden decir todo a todos y que todos pueden tener acceso a todo sin ningún tipo de respeto a, por ejemplo, los derechos de propiedad intelectual – no es sino el reverso de una sociedad fascista en la que sólo un grupo de personas se adjudica el derecho a hurgar en la memoria corporal y/o digital de los ciudadanos sin marco legal que los proteja tanto de la arbitrariedad estatal como del espionaje e intromisión sin su consentimiento. Pienso que la solución a este problema de la diferencia entre lo público y lo secreto (incluyendo lo privado) no ha de buscarse en un intento de creer que se pueda fijar definitivamente una línea de demarcación sino en mantener abierta la discusión política y académica que observe las razones por la cuales en determinadas situaciones sea conveniente mover la demarcación en uno u otro sentido. Lo básico en una sociedad democrática es que dicho debate sea público.

Raquel En estas contradicciones del mundo actual que justamente tu señalas no siempre es fácil navegar. Quiero evocar al respecto la figura de Alan Turing (1912-1954) que puede ser considerado uno de los padres de la Inteligencia Artificial y cuya vida se trama dramáticamente con el tema que nos convoca. Durante la segunda guerra mundial Turing formó parte del equipo de inteligencia que diseñó en Inglaterra una máquina llamada la 'Bomba' con la finalidad de explorar las combinaciones posibles generadas por la máquina codificadora alemana 'Enigma'.

Trabajó después en la Universidad de Manchester y en el programa MADAM (Manchester Automatic Digital Machine) que resultó ser el equipo de computación de mayor memoria construido hasta entonces. Pero su trabajo de descifrador de enigmas se acompañó después de la guerra de un descuido que le fue fatal. Turing denunció en la policía local un robo del que fue víctima, efectuado por un partenaire casual con el que había compartido la noche. Creyó que su homosexualidad podía ser pública y no midió las consecuencias sociales de sus declaraciones. Fue condenado a causa de su homosexualidad a un tratamiento o tortura, médico-farmacéutica equivalente a la castración. Turing se suicidó en 1954,

comiendo una manzana envenenada. Se dice que la manzana de Apple lo recuerda con un guiño. Esto para acentuar que el juego de las contradicciones en las que vivimos es un juego que a veces se torna peligroso y no puede ser jugado de modo ingenuo. El otro punto con el que quiero terminar para abrir a un diálogo más amplio es el de subrayar que estar aquí reunidos para debatir sobre estos temas, marca como acontecimiento el límite de los espacios virtuales y el irremplazable lugar de encuentro de los cuerpo vivos que se regocijan en el hablar y el escucharse unos a otros.

Rafael Y también son claros los límites de los encuentros corporales sobre todo viendo las posibilidades del intercambio de información digital como lo hemos venido haciendo en este diálogo transatlántico. Creo que el ensamblaje entre los mensajes digitales y el encuentro faz a faz es algo que caracteriza a las sociedades de la información en este siglo. Es justamente este ensamblaje el que crea nuevos desafíos éticos con respecto a la delimitación entre informaciones públicas e informaciones secretas sobre todo si recordamos que el adjetivo 'secreto' no es algo inherente a una información sino una adjudicación a una relación siendo 'información' a su vez una categoría de segundo orden es decir dependiente del sujeto o sistema que la percibe como tal. Las diversas paradojas de la sociedad de la información a las que nos hemos referido podrían sintetizarse con el término de *paradoja de Google*: la buscadora quiere hacer accesible a todos, ella sola, toda la información digital manteniendo secreto su algoritmo.

Agradecimiento

Los autores agradecen al Prof. Oscar Krütli (Provincia de Córdoba, Argentina) por su crítica a este texto.

Bibliografía

Allouch, Jean: Le sexe de la vérité. Paris: Cahiers de l'unebévue, Epel 1998.

Boneberg, Hemma: Geheimhaltung. En: Christoph Auffarth, Jutta Bernard, Hubert Mohr Ed.: Metzler Lexikon Religion. Stuttgart: Metzler 1999, Vol. 1, p. 460-462.

Capurro, Rafael: Ethik der Informationsgesellschaft. Ein interkultureller Versuch. 2006. Online: http://www.capurro.de/parrhesia.html

Foucault, Michel: Discourse and Truth: the Problematization of Parrhesia, 1983 Online: http://foucault.info/documents/parrhesia

Geffroy, Lucie: Blogs d'écrivains, au-delà de l'intime. En: Magazine littéraire, No. 11, Mars-Avril 2007, p. 27.

Derrida, Jacques: Mal d'archive, Paris: Galilée 1995.

Freud, Sigmund: Das Unbehagen in der Kultur. En ibid.: Fragen der Gesellschaft. Ursprünge der Religion. Frankfurt am Main: S. Fischer 1974, p. 191-270.

Freud, Sigmund y Fliess, Wilhelm: Briefe an Wilhelm Fliess. Frankfurt am Main, S. Fischer 1986.

Jullien, François: Le détour et l'accès. Stratégies du sens en Chine, en Grèce. Paris: Seuil 1995.

Jullien, François: Nourrir sa vie. À l'écart du bonheur. Paris, Seuil 2005.

Lacan, Jacques: Ecrits. Paris: Seuil, 1966.

Lacan, Jacques: Le Séminaire, VII, L'éthique de la psychanalyse. Paris: Seuil, 1986/1960, cap. XI.

Lacan, Jacques: Le Seminaire: D'un Autre à l'autre. Paris: Seuil 2006.

Lacan, Jacques: L'Unebévue, En: Revue de psychanalyse 2004, nº21. Paris: Epel.

Simmel, Georg: Das Geheimnis und die geheime Gesellschaft. En: ibid.: Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Frankfurt am Main, 1995. p. 383-455. http://socio.ch/sim/unt5a.htm

Strauss, Leo: La persécution et l'art d'écrire. Paris, Presses Pocket 1989 (orig. 1952).

Wittgenstein, Ludwig: Tractatus logico-philosophicus. Frankfurt am Main: Suhrkamp 1984.

Sami Coll:

The social dynamics of secrecy: Rethinking information and privacy through Georg Simmel

Abstract:

This article argues that Georg Simmel's ideas on secrecy can shed new light on current debates around the relevance or otherwise of privacy as a protection against surveillance interventions. It suggests an interactional approach to privacy, and considers it as a dynamic process which redefines the boundary between what information should be disclosed and what information should be concealed in every social interaction. Simmel argues that this "natural" process relies on the identification of the interlocutor: her psychological/emotional involvement in the relationship, her social position in society and the representation of her expectations. Recent empirical examples show that this interactional perspective may have the potential to reconcile differing privacy accounts, by linking theoretically different levels that are factually distinct: privacy as a collective fact, as a contextual integrity, and as an individual fact.

Agenda:

Author:

Dr. Sami Coll:

- Department of Sociology, University of Geneva, Switzerland
- ✉ socio@samicoll.com, 💻 www.samicoll.com

In 1906, German Sociologist Georg Simmel published a pioneering paper on secrecy in the American Journal of Sociology: 'The Sociology of Secrecy and of Secret Societies'. It was later revised and published in 1908 in his mother tongue as a chapter of *Soziologie: Untersuchungen über die Formen der Vergesellschaftung*, then retranslated to English and published in 1950 as *The Secret and the Secret Society*. At the beginning of the 20th century, the notion of privacy was not developed to the extent it is now, especially with respect to the emergence of the information society (Regan 2011, 497). However, the social dynamics of secrecy analysed in Simmel's writings appear to be similar to those that can be observed in the context of the information era. Indeed, Simmel suggests an "exploration of the role of information in social interactions" (Marx and Muschert 2009, 217). Focusing exclusively on the social dimensions of informational practice, Simmel avoids being drawn into an ethical position on how and/or whether information flows should be regulated. As such, Simmel's analysis does not reduce the richness of social reality to a duality between an emitter and a receptor, as it tends to be in data protection policies. For these reasons, I argue in this paper that Simmel's theory on secrecy is able to shed an intriguing light upon privacy and data protection debates.

1 The limits of privacy

1.1 Current debates about privacy

While most scholars agree that the privacy notion is vague and not rigorous enough to address issues relating to contemporary surveillance practices (Bennett 2008), disagreements emerge around how rights to a private life should be protected in cultures defined by ubiquitous surveillance. Traditional approaches still advocate for approaching privacy from the level of the individual (Bennett 2008; Bennett 2011a), arguing that there is a legislative regime already in place which can be exploited to provide citizenry protection (Bennett 2011b; Stalder 2011). Other scholars argue that the concept should be withdrawn and replaced with alternative values (like Gilliom 2011). I have previously described how privacy might be understood as a close ally of surveillance (Coll 2010). This is because the notion tends to be exploited by privileged groups to perpetuate forms of capital accumulation, much like the artistic critique was absorbed in the late 20th century by regimes concerned to maintain the political-economic status quo (Boltanski and Chiapello 2005). Certain scholars argue that in order to be more effective, privacy should be approached with a relational and/or contextual perspective (Nissenbaum 2009; Steeves 2009), whilst others contend that it should be transformed to become a more collective project (Regan 1995; Regan 2011; Gilliom 2011). Despite the indisputable importance of these approaches, the distinction between the relational/contextual perspective and the collective perspective is not always very evident.

1.2 An empirical perspective: The loyalty card programmes

My recent empirical research on people's attitudes to loyalty card programs attempts to move beyond often abstract theoretical discussions on the capacity of privacy legislation to protect individuals and populations from diverse forms of surveillance (Coll 2010). Results from this research show that there are – in the specific context of loyalty programmes – three different perspectives on privacy to consider. First, what might be understood as official and legal *informational privacy*. Upheld by various laws generated in the context of the information society, this form of privacy is generally viewed as a fundamental right which protects individuals from undesired intrusions and unlawful interference from the state, private companies, or simply other persons motivated by curiosity (Stalder 2002, 121). Second, *consumers' subjective privacy*, as consumers themselves define it, relates to a freedom of choice ideology, or the freedom of making decisions without being influenced by a third party. Third, *privacy as an everyday life experience* relates to the actual situations where actors feel that their privacy is being breached, particularly as a result of loyalty card programmes that collect, conserve and potentially analyse their personal data. My observations in a loyalty card call centre, for example, showed that consumers were more annoyed by the identity verification questions fielded by operators – although there are meant to protect their privacy – than by the company's storage of their personal data. On the contrary, consumers expect companies to retain their data. When consumers

contacted the same call centre to ask for a hardcopy of a lost warranty, they were not pleased to discover that in order to protect their privacy the database did not contain details of their recent purchases.

An important question emerges at this point: how is it possible to generate an approach to privacy as a form of protection against the effects of massive data collection and processing if there is no agreement among legislators or individuals on its constitutive form? As shown, consumers themselves display much ambivalence towards privacy. Most of the time, their verbalized definitions do not correspond with how they endure privacy breaches in everyday life. My research showed that the *informational self-determination principle* guiding data protection laws – i.e. that every person is supposed to be a proactive guarantor of her own privacy (using freedom of access legislation to correct or erase inaccurate information), is seriously challenged by the scale of contemporary surveillance operations and individuals' general lack of knowledge on how, why and from where data is collected.

2 Privacy as a social interaction: Simmel's work on secrecy

2.1 From secrecy to privacy

Simmel's work on secrecy – and using it to frame an approach of privacy as an interactional and social property – offers a novel perspective from which we might move beyond existing contradictions and paradoxes.

First, Simmel reminds us that a society with "full publicity" (Simmel 1950a, 330) would not be stable and would rupture the interaction order, a similar position to that adopted by Solove: "A society without privacy protection would be suffocating, and it might not be a place in which most would want to live" (Solove 2007, 762). Simmel then contends that "one can never know another person *absolutely*, which would involve knowledge of every single thought and mood. Nevertheless, one forms some personal unity out of those of his fragments in which alone he is accessible to us. This unity, therefore, depends upon the portion of him which our standpoint permits us to see" (Simmel 1950a, 308). Indeed, the information sought by a person on another can come from "many sources of information (…) and many carriers" (Goffman 1959, 1).

Finally, Simmel speaks of secrecy as "the feeling (…) that an ideal sphere lies around every human being. Although differing in size in various directions and differing according to the person with whom one entertains relations, this sphere cannot be penetrated, unless the personality value of the individual is thereby destroyed" (Simmel 1950a, 321). In other words, there is no doubt that the "ideal sphere" described by Simmel is precisely what is now commonly known as the sacrosanct realm of "privacy".

It is in Simmel's thick description reported above where overlaps between his secrecy reflections and privacy debates become evident, specifically because the "ideal sphere" cannot be seen as a static "bubble" which would supposedly contain private or sensitive data. The "ideal sphere" instead emerges from dynamic social interactions and the boundary between private and public is continuously in flux.

2.2 The dynamics of secrecy/privacy

Much like communication, secrecy, as a social dynamic, guarantees a society's social cohesion. Any social relation requires a balance between disclosure and concealment, and this balance needs to be negotiated in each social interaction: "the secret is a form which constantly receives and releases contents: what originally was manifest becomes secret, and what once was hidden later sheds its concealment" (Simmel 1950a, 335). Information which might be perceived as private in one context can be disclosed in another where it is not considered such. For example, a customer in a bakery would most probably not feel transgressed by someone wishing to know her favourite bread variety, but she might experience discontent or discomfort if asked the size of her panties. In contrast, in a clothes shop, providing information on size is mandatory to the provision of a good service, while being asked about favourite bread type might be deemed inappropriate,

and potentially induces a feeling of privacy invasion. Thus, the context of the social interaction defines the relevance of the informational disclosure as well as its (in)appropriateness.

While this theoretical model is well suited in the context of a face-to-face interaction, it becomes more complex when it involves an interaction between an individual and an institution, whether public or private. The image of the institution can be mixed-up with the person representing the institution during an interaction. The definition of the boundary between what information should be transmitted (considered public in this context) and what information should be concealed (private) will, naturally, depend on what service the person expects of the institution, but also on the personality and projected judgements of the employee in charge of providing the service. In my research, feelings that privacy had been breached were expressed in very concrete situations. They involved the personal characteristics of an employee rather than the ones of the organization. For example, when a young man at customer services asks a middle-aged woman for her date of birth, the woman feel discomfort by the fact the employee is younger, and not because the company can possibly use her date of birth for marketing purposes. Indeed, interactions remain in large part interactions between two human beings even in the contextual parameters of an organisation: "Every relationship between persons gives rise to a picture of each in the other; and this picture, obviously, interacts with the actual relation" (Simmel 1950a, 309). This image is partly based on the organizational setting but in large part emerges as an outcome of the quality of interaction shared between interlocutor and individual.

2.3 The spontaneous regulation of the flow of information

Simmel considers the dynamic process of agreeing and upholding the boundary between private and public information as a "natural" process (Simmel 1950a, 311–312). The term "natural" is probably inappropriate as this process is in fact historically and normatively contingent. It is integrated through the socialisation of individuals into particular codes of conduct (DePaulo et al. 2003). The decision to disclose or conceal information is made spontaneously and subconsciously (this is actually what Georg Simmel meant by the "natural" or organic framing of this dynamic). On the one hand, we can reasonably assume that the social and spontaneous nature of this process permits mutually regulated flow of information in the context of everyday life and face-to-face relationships. On the other hand, when it comes to regulating the flow of personal information through digitalized devices, this spontaneous ability may no longer be available as a checking device.

This dynamic process becomes more complex when the interlocutor is virtual and thus more difficult to clearly discern. Indeed, the "natural" regulation of informational flow as described by Simmel is based on the fact that the interlocutor is clearly identifiable. For example, consider the case of completing a website application form: the identification of the interlocutor and one's capacity to build an appropriate image of it cannot be made as in a face-to-face interaction. In this case, a set of important social rules and conventions are absent. In contrast, consider the situation of completing a form at a customer service desk. Here, it is the employee and not the organization that is clearly identifiable. The boundary tends to be delimited according to the identification and the evaluation of the employee's conduct rather than that of the company more generally.

In the case of social network sites like Facebook, it is not easy to clearly identify the interlocutor neither. Is it a group of "friends", a "friend" of a "friend" or a future "friend" who will have access to previously published data? Will it be anyone registered on the network? In such a context, evaluating the receptor of a message (a picture, a status, a video, etc.) is extremely complex, if not impossible. Thus, the "natural" process mentioned by Simmel is not able to conceal the risks of an inappropriate disclosure of sensitive information. However, no substitute for spontaneous regulation is currently available. Therefore, this regulation principle continues to govern the disclosure of data in the current information age, and this approach has several limitations in terms of ensuring an order that is mutually constituted.

3 Conclusion

An interactional approach to privacy, based on Simmel's theory of secrecy, enables us to understand paradoxical situations. On the one hand, measures meant to protect an individual's privacy are the very mechanisms which produce a feeling of invasion. On the other hand, such reactions do not occur in situations where they are expected. It also reminds us that the relationship between an individual and an institution is often mediated by an employee who proves decisive in deciding the boundary between what to conceal and what to disclose.

Several important issues need to be borne in mind. First, the notion of secrecy (that is to say, privacy) always implies an "Other" (Marx and Muschert 2009, 223). An "ontological" privacy can only exist in relation to an interlocutor. Second, secrecy dynamics are relational and context-dependent. The definition of the context involves many parameters: the identification of the interlocutor, her role in the institution, her psychological/emotional involvement in the relationship, her social position in the society, her expectation (or, rather, our projected view of her expectations), etc.

According to Simmel, interactions are at the origin of social structures of power (Simmel 1950b; Coser 1977). The social dynamics of secrecy are not an exception. Rather than being a social fact in which we should protect an individual's privacy and liberty, information (and its partner, secrecy) is thus constitutive of the individual and her social relations. In other words, when a certain boundary between disclosure and concealment is repeated through certain types of social relations, it becomes a structure, and then a collective fact. As the capacity to withhold specific information becomes a commodity constitutive of power and social stratification (Simmel 1950a, 338), secrecy (which is, again, in Simmel's language, privacy) has an important collective implication, one which is defended by those scholars wishing to retain privacy as a collective good (see Westin 2003; Regan 1995; Regan 2011).

Adopting Simmel's theory on social interactions and on secrecy enables an interesting approach to be built around the sociology of intimacy and privacy. Such an approach may have the potential to reconcile existing privacy debates, and link different privacy forms that are factually distinct: privacy as a collective fact, as a contextual integrity and as an individual fact. It can, for example, lead us to a better understanding of the social dynamics and the modalities of transparency operating in and across social networks (Coll, Glassey, and Balleys 2012).

References

Bennett, Colin J. 2008. The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge, MA: MIT Press.

———. 2011a. "In Defence of Privacy: The Concept and the Regime." Surveillance & Society 8 (4): 485–496.

———. 2011b. "In Further Defence of Privacy..." Surveillance & Society 8 (4): 513–516.

Boltanski, Luc, and Eve Chiapello. 2005. The New Spirit of Capitalism. London, New York: Verso Books.

Coll, Sami. 2010. "Consommation Sous Surveillance: L'exemple Des Cartes De Fidélité". PhD diss. Genève: Université de Genève, Faculté des sciences économiques et sociales.

Coll, Sami, Olivier Glassey, and Claire Balleys. 2012. "Building Social Networks Ethics Beyond 'privacy': a Sociological Perspective." International Review of Informational Ethics 16.

Coser, Lewis. 1977. Masters of Sociological Thought: Ideas in Historical and Social Context. New York: Harcourt Brace Jovanovich.

DePaulo, Bella M., Chris Wetzel, R. Weylin Sternglanz, and Molly J. Walker Wilson. 2003. "Verbal and Nonverbal Dynamics of Privacy, Secrecy, and Deceit." Journal of Social Issues 59 (2): 391–410.

Gilliom, John. 2011. "A Response to Bennett's 'In Defence of Privacy'." Surveillance & Society 8 (4): 500–504.

Goffman, E. 1959. The Presentation of Self in Everyday Life. New York: Anchor Books, Doubleday.

Marx, Gary T., and Glenn W. Muschert. 2009. "A Legacy and Inheritance for the Sociology of Information." In Soziologie Als Möglichkeit: 100 Jahre Georg Simmels Untersuchungen Über Die Formen Der Vergesellschaftung, ed. Cécile Rol and Christian Papilloud, 217–233. Wiesbaden, Germany: VS Verlag für Sozialwissenschaften.

Nissenbaum, Helen. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Standford: Stanford University Press.

Regan, Priscilla M. 1995. Legislating Privacy. Chapel Hill & London: The University of North Carolina Press.

———. 2011. "Response to Bennett: Also in Defence of Privacy." Surveillance & Society 8 (4): 497–499.

Simmel, Georg. 1950a. "The Secret and the Secret Society." In The Sociology of Georg Simmel,ed. Kurt H. Wolff, trans. Kurt H. Wolff, 305–376. Glencoe Ill.: Free Press.

———. 1950b. The Sociology of Georg Simmel. Ed. Kurt H. Wolff. Trans. Kurt H. Wolff. Glencoe Ill.: Free Press.

Solove, Daniel J. 2007. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." San Diego Law Review 44: 745–772.

Stalder, Felix. 2002. "Opinion. Privacy Is Not the Antidote to Surveillance." Surveillance & Society 1 (1): 120–124.

———. 2011. "Autonomy Beyond Privacy? A Rejoinder to Bennett." Surveillance & Society 8 (4): 508–512.

Steeves, Valerie. 2009. "Reclaiming the Social Value of Privacy." In Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, ed. Ian Kerr, Carole Lucock, and Valerie Steeves, 193–208. New York: Oxford University Press.

Westin, Alan F. 2003. "Social and Political Dimensions of Privacy." Journal of Social Issues 59 (2): 431–453.

Meg Leta Ambrose:

You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship

Abstract:

The right to be forgotten is a proposed legal response to the potential harms caused by easy digital access to information from one's past, including those to moral autonomy. While the future of these proposed laws is unclear, they attempt to respond to the new problem of increased ease of access to old personal information. These laws may flounder in the face of other rights and interests, but the social values related to moral autonomy they seek to preserve should be promoted in the form of widespread ethical information practices: information stewardship. Code, norms, markets, and laws are analyzed as possible mechanisms for fostering information stewardship. All these mechanisms can support a new user role, one of librarian - curator of digital culture, protector of networked knowledge, and information steward.

Agenda:

Author:

Meg Leta Ambrose:

- ATLAS Institute, University of Colorado, Boulder, 1125 18th St., 80309-0320 Boulder, Colorado
- ☎ + 1 - 303-735-4577, megleta@gmail.com, www.megleta.com

ISSN 1614-1687

1 Introduction

We size each other (and ourselves) up through online search engines. Universities, employers, and potential romantic partners search users to discover what has not been included in the initial disclosure. Perhaps this new information practice is why 94% of parents and 94% adults feel that after a period of time, an individual should have the ability to have personal information held by search engines, social networking sites, or marketing companies deleted.[1] It is difficult to change when one cannot move beyond the past. The Internet changes access to the past and this new form of access may limit the growth and development of the individual. Facebook Timeline feels like a privacy invasion to many because old information about us has not been recalled with ease or great detail in the past. This paper details these issues and examines proposed responses to threats to moral autonomy posed by personal information accessible online. After briefly introducing the right to be forgotten, I discuss research on information persistence to properly frame the problem. I then propose wide-spread information stewardship to support responsible retention of information to prevent stagnation of the self in the Internet Age.

2 Information Landscape and Moral Autonomy

In an age when "[y]ou are what Google says you are," [2] expecting parents search prospective names to help their kids retrieve top search results in the future, and only a few rare parents want their children to be "lost in a virtual crowd,"[3] even in light of the notion that "[l]ife, it seems, begins not at birth but with online conception[, a]nd a child's name is the link to that permanent record."[4] Changes in the storage, disclosure, and retrieval of information have spurred governmental initiatives to prevent injustices that may arise from black marks on that "permanent record," the right to be forgotten being the most prominent.

2.1 Moral Ethics and Fluidity of the Self

Shaping and maintaining one's identity is "a fundamental interest in being recognized as a self-presenting creature."[5] The person is a dynamic pursuit of moral improvement and "cannot be identified… as something limited, definite, and unchanging."[6] When information about an individual is available in a way that she did not intend, this pursuit is disrupted. "The conception of the person as being morally autonomous, as being the author and experimentator of his or her own moral career, provides a justification for constraining others in their attempts to engineer and directly or indirectly shape the subject's identity."[7]

2.2 The Right to be Forgotten and the "Eraser Button"

The right to be forgotten is a legal response to threats to the dynamic self from modern information technology and practices. The European Commission for Justice, Fundamental Rights and Citizenship, Viviane Reding, has declared the right a pillar of the new Data Protection Directive, currently being redrafted. Although conceived as a right, value, interest, virtue, and ethical principle, I will refer to the prevention of self-stagnation by limiting access to or deleting information that has aged a certain term as a right. The roots of

[1] Zogby International Poll, http://www.ftc.gov/os/comments/privacyreportframework/00457-57996.pdf (2010).

[2] "You Are What Google Says You Are," Wired. Feb. 11, 2009.

[3] Allen Salkin, "What's in a Name? Ask Google," The New York Times, Nov. 25, 2011.

[4] *Id.*

[5] J.D. Velleman, *The Genesis of Shame*, 30 Philosophy and Public Affairs 27-52 (2001).

[6] Jeroen van den Hoven, *Information Technology, Privacy, and the Protection of Personal Data*, in Information Technology and Moral Philosophy 319 (2008).

[7] *Id.*, at 317.

the right to be forgotten are found in the prohibition of media disclosure of information related to criminal activity after the defendant has been sentenced. Being forgotten (the right to have third parties forget your past) and forgetting (the right to avoid being confronted with your past) are both embraced by the French concept *oubli*, oblivion, which denotes a negative right that others abstain from remembering one's past as well as a subjective right of the individual to control his past and future. While a draft of the European Union Data Privacy Directive has been released, the contours of the right to be forgotten have not yet been defined. In the meantime, Google has challenged the Spanish Data Protection Agency order to remove URLs from its index that point to personal information the Agency has determined should be forgotten. A similar proposal has been made in the "Do Not Track Kids" legislation, an amendment to the Child's Online Privacy Protection Act.[8] The bill includes an "eraser button" to eliminate the publicly available personal information of children.[9]

2.3 Content Persistence

Contrary to popular notions, Web content is quite ephemeral. Information online is not permanent for a number of reasons including media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures.[10] Information also loses value over time because it may become an inaccurate representation of the present, de-contextualized, and/or irrelevant.[11] Recent work suggests, albeit tentatively, that data is becoming *less* persistent over time; for example, Gomes and Silva studied the persistence of content between 2006 and 2007 and discovered a rate of only 55% alive after 1 day, 41% after a week, 23% after 100 days, and 15% after a year.[12]

If access is to be manipulated in order to protect moral autonomy, the landscape must be accurately portrayed. Information that remains online may become an inaccurate reflection of the individual as he or she changes the access to which may result in significant limitations and loss of opportunities. Information is not permanent no matter the medium, and digital mediums have their own weaknesses. Thus, without principled information practices, valuable information may easily disappear while harmful, low value information may remain longer than socially deemed appropriate.

3 Information Stewardship

3.1 Maternalistic Privacy

People once asked other people for answers. Now we ask machines, but these machines are human-created to meet human goals. At the Time & Bits conference in 1998, the attendees asked "Who is responsible?" "There are serious questions as to who will take responsibility for making digital information persist over time."[13] I propose that users take responsibility of this space as stewards of knowledge produced, used, collected, and organized online. Information stewardship is a responsibility imparted on database managers for the information they are entrusted with. Extending this ethic is a maternal, as opposed to paternal, form of privacy protection. It does not proscribe specific behaviour that is best for users or prohibit any specific

[8] H.R. 1895: Do Not Track Kids Act of 2011.

[9] H.R. 1895, Sec. 7 (2011).

[10] Henry M. Gladney, *Preserving Digital Information,* 10 (2007).

[11] R. Glazer, *Measuring the Value of Information: The Information-Intensive Organization*, 32(1) IBM Systems Journal 99, 101 (1993).

[12] Daniel Gomes and Mario J. Silvia, Modeling Information Persistence on the Web, Proceedings of the 6th International Conference on Web Engineering 1 (2006).

[13] Margaret MacLean, Ben Davis, Getty Conservation Institute, Time & Bits: Managing Digital Continuity, 19 (1998).

behaviour, but encourages users to nurture the space for long-term benefits and emphasizes the Web as a whole and as part of our social existence.

Data managers have long been stewards of the information they have been entrusted and responsible to maintain the timeliness, accuracy, and access control of the data.[14] These information stewards manage data over its lifecycle by accounting for the changing value of information from conception to disposition.[15] These basic principles underscore widespread information stewardship, which can be addressed and promoted through a number of mechanisms including markets, norms, code, and laws.[16] These mechanisms may simply allow for personal information to be less accessible over time or actively practice limiting access to or editing personal information in an attempt to minimize harm while retaining valuable substance.

3.2 Markets

The market has answered the call for reputation tarnish. Companies like Reputation.com, TrueRep.com, and IntegrityDefender.com offer services to repair your reputation and hide your personal information. On the "Suppress Negative Content Online" page of Reputation.com, the site explains that "You're being judged on the Internet," "The Internet never forgets," "The truth doesn't matter," and that you are "Guilty by association."[17] These may seem dramatic, but for those that live with a nasty link on the first page of a Google search for their name, it probably feels very accurate. Reputation.com apparently, works; it claims a 99% success rate (although any bad reviews would likely be buried).

The fact that these businesses are successful suggests that there is a market of users with injured online reputations seeking redress, that the Internet has little integrity to preserve, and that drafting laws to create hurdles to access may be unnecessary. Today, only those with means can remove themselves from the record of the Internet and those less powerful can only hope for an opportunity to explain their digital dirty laundry. While it may be appealing to demonize the "privacy for a price" approach in favor of one based on privacy for all, these services provide privacy from past negative information, a very complicated task, starting at the low price of $15 per month.

This form of intervention may promote the goals of reputation rehabilitation, but it is not information stewardship. The easiest way to make negative information less accessible is to bury it under highly ranked positive information - and lots of it. Google results can be seen as context. It is what the Web has on a user and what is the most important about them. While a reputation service can add content that adds context, it is not necessarily more accurate, relevant or valuable. Additionally, this does not offer real seclusion or the feeling of being left alone, or any other privacy definition related to autonomy. If a user is interested in seclusion, paying for a service that will plaster information about them all over the Internet, does not support their goals of regaining a private existence. If a user seeks to control information communicated about him or her, reacting to pressure to fill the Web with positive information in order to place a piece of information back in a sphere of privacy is more like strong-arming a user than empowering him or her with privacy.

The market also addresses any information a client desires. It can suppress new, old, true, false, uncontextualized, wholly fair, public or private information. In other words, these services "edit" the Internet, creating search barriers to valuable, as well as valueless, information. Relying on services that game the system reinforces the Internet as something to play with as opposed to a source of knowledge, not the goal that many have for the Internet. A real market response to information stewardship would be a movement of traffic toward up-kept content.

---

[14] Richard A. Spinello, Case Studies in Information and Computer Ethics, 7 (1997).

[15] David G. Hill, Data Protection: Governance, Risk Management, and Compliance, 57 (2009).

[16] Those set forth by Lawrence Lessig in Code (1999).

[17] "Suppress Negative Content Online: ReputationDefender: Reputation.com," https://www.reputation.com/reputationdefender.

3.3 Code

In early November, 2011, Google announced that it would be making search results "fresher and more recent."[18] The tweak affects about 35% of all searches.[19] The algorithm is now better designed to determine if a user wants to find fresh information (the score of a big game currently happening or when a concert will be coming to the area) or older information (the capital of a state or recipe for bread). How the new algorithm will impact searches for individuals is unclear, but the tailoring of search results to better account for fresh information where appropriate displays the capabilities of search engines to account for the low value of old information.

Google's main competition for the freshest information is Twitter. Twitter does not show old search results. For instance, typing in #obama2008 retrieves only 2 Tweets, both which also include the hashtag #obama2012 and were posted in the last few days. On the other hand, Twitter displays all publicly available Tweets for a user if you select their profile page. All publicly available Tweets are also collected by the Library of Congress, but are only accessible to "known researchers." These distinctions matter. Varying levels of accessibility, or the ease of retrieval, create barriers similar to those of a paper-based record society. These variations, like the old barriers, are not rooted in privacy, but information value. In order to provide the most value, information systems are managed.

4Chan, a notorious chat forum not for the faint of heart, maintains content ephemerality with thread expiration. As new threads are added, old ones get pushed down. The thread is removed permanently when it is pushed to the bottom of the fifteenth page and retrieves a "Page Not Found" error when its URL is entered. However, the thread is bumped back to the top when a user replies to the thread.[20]

These above are just a few examples of code-supported information stewardship, but the technologies need not be complex. Reminders that the information we contribute still exists and may be harmful or useful could support a more valuable online experience. For instance, after a set amount of time, a reminder would appear in email or upon sign in to a service that the user posted information identifying another individual, that the information has been crawled, and ask whether the user would like to anonymize, unindex, delete, or leave the content unchanged. Notices of information loss could also promote the preservation of possibly important information. Site owners could choose to archive the site with archive.org or another institution or allow important information to remain once long term consequences have been considered.

3.4 Norms

Shifts in norms have been offered as the solution to lingering personal information retrievable online. The idea is that we will all be used to seeing indiscretions online and will not judge people too harshly for those exposed indiscretions - after all, deep down we know no one is perfect. The opposite is also possible - norms of non-disclosure and "normalization." This section examines examples of norms related to the necessity of the identification of individuals to contribute valuable content.

The Star Wars Kid Wikipedia page does not include the name Ghyslain Raza. This is no accident;[21] Wikipedia adheres to a Biographies of Living Persons Policy which includes a presumption in favor of privacy.[22]

---

[18] "Official Google Blog: Giving Your Fresher, More Recent Search Results," Nov. 3, 2011, http://insidesearch.blogspot.com/2011/11/giving-you-fresher-more-recent-search.html.

[19] *Id.*

[20] For a more detailed study of 4Chan's content ephemerality see M.S. Bernstein, A. Monroy-Hernández, D. Harry, P. André, K. Panovich, and G. Vargas, *4chan and /b/: An analysis of anonymity and ephemerality in a large online community*, In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain (2011).

[21] "Talk: Star Wards Kid – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

[22] "Wikipedia: Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

> *"Caution should be applied when identifying individuals who are discussed primarily in terms of a single event. When the name of a private individual has not been widely disseminated or has been intentionally concealed, such as in certain court cases or occupations, it is often preferable to omit it, especially when doing so does not result in a significant loss of context... Consider whether the inclusion of names of private living individuals who are not directly involved in an article's topic adds significant value."*

This is probably a good rule for all Internet contributions, but unfortunately, these efforts are somewhat wasted. Google search results for Ghyslain Raza return the Star Wars Kid Wikipedia as the most relevant result, highlighting the need for a more cohesive approach to old information.

The archival profession has developed and maintained a Code of Ethics to guide their practices while protecting privacy rights of donors and those that are the subjects of records. They "respect all users' right to privacy by maintaining the confidentiality of their research and protecting any personal information collected about them in accordance with the institution's security procedures."[23] Like the Internet community, the archival community is faced with a competing access principle: "Archivists strive to promote open and equitable access to their services and the records in their care without discrimination or preferential treatment, and in accordance with legal requirements, cultural sensitivities, and institutional policies."[24] With more and more archives being digitized, these decisions become more important. For instance, should diaries be digitized and accessible by anyone when they contain sensitive material about a person that is still alive? Diaries are not meant to be read by anyone but the writer and perhaps descendants, but valuable historical and cultural information has been extracted from diaries such as that of Anne Frank, Virginia Woolf, George Washington, Thomas Jefferson, William Bradford, and Sylvia Plath. The Internet Archives exclusion policy follows the guidelines set forth for traditional archives and clearly lays out the appropriate response to specific types of removal requests.[25]

Public Resource, a site that republishes court documents, evaluates and grants requests from individual's identified in the cases to remove the case retrieval by Google.[26] The documents are public records, but Public Resource will add a robots.txt file so that ethical crawlers will not index the page, and in turn, will not be presented in search engine results. The information is not deleted and still accessible through the site, but not to through a search. The above represent the norms or practices of content sources that have some sort of hierarchy and established policies, but similar ethics exist across the decentralized Internet as well. While information may be vital to capturing cultural history, identification may not. These entities protect the integrity of the information while providing a degree of privacy to the subject.

3.5 Law

When content falls through the net of the above safeguards, the law may need to step in. Some content need not rely on decay because it is inherently damaging and dangerous - toxic (e.g., social security numbers or health information). If the above means do not help the subject, perhaps legal recourse is appropriate. We must be willing to assess the value of the information, the value added by identification of the subject, and the adjustments to information we are willing to make. However, if the information supports public safety or consumer protection or identification of the subject is *still* central to the debate, access manipulation would not be appropriate.

When information is no longer newsworthy or of public interest, which can be supported by using simple tools like Google Trend and hit counts, information law is in somewhat new territory. Many victories over

---

[23] "Code of Ethics for Archivists," Society of American Archivists, SAA Council Approval/Endorsement Date: February 2005 http://www2.archivists.org/standards/code-of-ethics-for-archivists.

[24] *Id.*

[25] "The Internet Archive's Policies On Archival Integrity and Removal," drafted Dec. 13-14, 2002 http://www2.sims.berkeley.edu/research/conferences/aps/removal-policy.html.

[26] "Why is My Court Case on the Internet?" Public.Resource.Org, https://public.resource.org/court_cases.html.

the First Amendment have been won with the blow of newsworthiness, but newsworthiness is not impenetrable and has not always trumped privacy claims. Although *Sidis v. F-R Publishing Corp* is a classic case that illustrates how a broad definition of newsworthiness leaves little left of the privacy tort of intrusion and a community standard of decency.[27] The Second Circuit explained that it could not confine "the unembroildered dissemination of facts"[28] unless the facts are "so intimate and so unwarranted in view of the victim's position as to outrage the community's notion of decency."[29] The idea that newsworthiness should protect all truthful information was flatly rejected by the Ninth Circuit in *Virgil v. Time, Inc.*:

> *"To hold that privilege extend to all true statements would seem to deny the existence of 'private' facts, for if facts be facts -- that is, if they be true -- they would not (at least to the press) be private, and the press would be free to publicize them to the extent it sees fit. The extent to which areas of privacy continue to exist, then would appear to be based on rights bestowed by law but on the taste and discretion of the press. We cannot accept the result."*[30]

Both cases resulted in losing plaintiffs and unscathed defendants who were allowed to expose the private idiosyncrasies of the subjects; the facts were "simply not offensive to the degree of morbidity or sensationalism."[31]

The "zone of privacy surrounding every individual" recognized by the Supreme Court has not been carved out, but there are instances in which the court has upheld privacy in the face of expression. For example in *Melvin v. Reid*, the movie depiction of a former prostitute's real-life involvement in a murder trial impinged the successful rehabilitation of the woman and overpowered the public's interest in her past. However, since *Time, Inc. v. Hill* (1967), the First Amendment has been the predominant and determining factor in these disputes. Since then, few cases have been successful and the false light tort has dwindled to just about nothing. Deference to journalists to determine what is newsworthy and assurance that the long tail of the Internet creates an audience for everything makes for a very convoluted notion of newsworthiness as a standard for the proper dissemination of private information.

Some courts have scrutinized the individual private facts disclosed and offered plaintiffs anonymity. In *Barber* the court explained that "[w]hile plaintiff's ailment may have been a matter of some public interest because unusual, certainly the identity of the person who suffered this ailment was not."[32] The Tenth Circuit adopted a "substantial relevance" test, meaning that the individual must be substantially relevant to the published content. In *Gilbert v. Medical Econ. Co.*, the court stated that some facts are indeed beyond the sphere of legitimate public interest:

> *"Even where certain matters are clearly within the protected sphere of legitimate public interest, some private facts about an individual may lie outside that sphere... [T]o properly balance freedom of the press against the right of privacy, every private fact disclosed in an otherwise truthful, newsworthy publication must have some substantial relevance to a matter of legitimate public interest."*[33]

The newsworthiness test established by these courts reinforces the notion that just because a story is of legitimate public concern does not mean that the plaintiff's identity is necessary to disclose. A more common judicial response is reflected by the court in *Shulman v. Group W. Productions, Inc.*, which refused to make

---

[27] *Sidis v. F-R Publishing Corp.*, 113 F.2d 806, 808 (2d Cir. 1940).

[28] *Id.*

[29] *Id.*

[30] *Virgil v. Sports Illustrated*, 527 F.2d 1122, 1128 (9th Cir. 1975).

[31] *Virgil v. Sports Illustrated*, 424 F. Supp. 1286 (S.D. 1976).

[32] *Barber v. Time, Inc.*, 159 S.W.2d 291, 295 (Mo. 1942).

[33] *Gilbert v. Medical Econ. Co., 665 F. 2d 305, 307-308 (10th Cir. 1981).*

this determination regarding a woman who was identified by the news in association with a horrendous car crash.[34] The court stated:

> *"That the broadcast could have been edited to exclude some of Ruth's words and images and still excite a minimum degree of viewer interest is not determinative. Nor is the possibility that the members of this or another court, or a jury, might find a differently edited broadcast more to their taste or even more interesting. The courts do not, and constitutionally could not, sit as superior editors of the press."*[35]

The most relevant principle expressed by the Supreme Court related to privacy, access, and time came in 1989 when it decided an issue surrounding reporters' Freedom of Information Act ("FOIA") requests for criminal history records of individuals involved in organized crime and a corrupt congressman from the FBI.[36] In *DOJ v. Reporters for Freedom of the Press*, the Court outlined a concept of "practical obscurity" for interpreting FOIA disclosures that fell under the privacy protections in Exemptions 6 and 7(C).[37] The "practical obscurity" concept "expressly recognizes that the passage of time may actually increase the privacy interest at stake when disclosure would revive information that was once public knowledge but has long since faded from memory."[38]

When confronting old information, the U.S. could attempt to draft a law that mirrors the right to be forgotten, based on the decay of newsworthiness attributed to information. There are pieces of case law that provide excellent foundations to build a privacy claim to remove or alter past information. Or the U.S. could rely on the above nudges from markets, norms, and code to support victims of the digital scarlet letter. The U.S. legal system, however, is not currently suited to force the hand of content creators or ISPs to enforce a right to alter truthful information, or its access points, distributed online. What the law can easily offer is context. In addition to the above-mentioned tools, the legal community could update an "outdated" legal claim: false light. An immense problem with negative information online is that it is often devoid of context, and therefore, misleading. Misleading information is something the U.S. legal system has experience with, albeit not much recent experience.

While false light has been called duplicative[39] and outdated,[40] thirty-one states allow the cause of action and ten have rejected it. However, in 2008 the Missouri Court of Appeals recognized that the tort may have new life in the digital age:

> *"As a result of the accessibility of the internet, the barriers to generating publicity are quickly and inexpensively surmounted. Moreover, the ethical standards regarding the acceptability of certain discourse have been diminished. Thus, as the ability to do harm grows, we believe so must the law's ability to protect the innocent."*[41]

False light claims that offer the plaintiff harmed by old information found online should be the simple addition of a timeframe. When someone suffers the financial, social, or personal harms of truthful information from their past, a false light claim would ensure that the information marked as old. Requiring at minimum a time stamp of when the content was created would allow technology to be layered on top of the added

---

[34] *Shulman v. Group W. Productions, Inc.*, 955 P. 2d 469 (Cal. 1998).

[35] *Id.*

[36] *DOJ v. Reporters for Freedom of the Press*, 489 U.S. 749 (1989).

[37] *Id.*

[38] Department of Justice Guide to the Freedom of Information Act 2009, 579 available at http://www.justice.gov/oip/foia_guide09/exemption7c.pdf, *citing DOJ v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, 767 (1989) ("[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even when the information may at one time have been public.").

[39] *Jews for Jesus, Inc. v. Rapp*, 997 So. 2d 1098, 1100 (Fla. 2008).

[40] *Denver Publ'g Co. v. Bueno*, 54 P.3d 893 (Colo. 2002).

[41] *Meyekord v. Zipatoni Co.,* 276 S. W.3d 319, 325 (Mo. Ct. App. 2008).

information to promote norms for those interested. For instance, a search for an individual could be limited to content time stamped within the last 5 years. A subject should be able to demand that old information be marked as such as to not mislead potential viewers. A false light claim for identifying information that is void of the context of time promotes the goals of information stewardship and is legally, socially, and technologically feasible.

References

Barber v. Time, Inc., 159 S.W.2d 291, 295 (Mo. 1942).

M.S. Bernstein, A. Monroy-Hernández, D. Harry, P. André, K. Panovich, and G. Vargas, 4chan and /b/: An analysis of anonymity and ephemerality in a large online community, In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain (2011).

"Code of Ethics for Archivists," Society of American Archivists, SAA Council Approval/Endorsement Date: February 2005 http://www2.archivists.org/standards/code-of-ethics-for-archivists.

Denver Publ'g Co. v. Bueno, 54 P.3d 893 (Colo. 2002).

Department of Justice Guide to the Freedom of Information Act (2009).

DOJ v. Reporters for Freedom of the Press, 489 U.S. 749 (1989).

Gilbert v. Medical Econ. Co., 665 F. 2d 305, 307-308 (10th Cir. 1981).

Henry M. Gladney, Preserving Digital Information (2007).

David G. Hill, Data Protection: Governance, Risk Management, and Compliance, 57 (2009).

R. Glazer, Measuring the Value of Information: The Information-Intensive Organization, 32(1) IBM Systems Journal 99, 101 (1993).

Daniel Gomes and Mario J. Silvia, Modelling Information Persistence on the Web, Proceedings of the 6th International Conference on Web Engineering 1 (2006).

Lawrence Lessig, Code (1999).

Jeroen van den Hoven, Information Technology, Privacy, and the Protection of Personal Data, in Information Technology and Moral Philosophy (2008).

Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1100 (Fla. 2008).

Internet Archive Frequently Asked Questions http://www.archive.org/about/faqs.php#29.

"The Internet Archive's Policies On Archival Integrity and Removal," drafted Dec. 13-14, 2002 http://www2.sims.berkeley.edu/research/conferences/aps/removal-policy.html.

Margaret MacLean, Ben Davis, Getty Conservation Institute, Time & Bits: Managing Digital Continuity, (1998).

Meyekord v. Zipatoni Co., 276 S. W.3d 319, 325 (Mo. Ct. App. 2008).

"Official Google Blog: Giving Your Fresher, More Recent Search Results," Nov. 3, 2011, http://insidesearch.blogspot.com/2011/11/giving-you-fresher-more-recent-search.html.

Lisa Rein, "Brewster Kahle on the Internet Archive and People's Technology," O'Reilly P2P.com http://openp2p.com/pub/a/p2p/2004/01/22/kahle.html.

Richard A. Spinello, Case Studies in Information and Computer Ethics, 7 (1997).

"Suppress Negative Content Online," ReputationDefender, https://www.reputation.com/reputationdefender.

Allen Salkin, "What's in a Name? Ask Google," The New York Times, Nov. 25, 2011.

Shulman v. Group W. Productions, Inc., 955 P. 2d 469 (Cal. 1998).

Sidis v. F-R Publishing Corp., 113 F.2d 806, 808 (2d Cir. 1940).

"Talk: Star Wards Kid – Wikipedia, the free encyclopaedia," http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

J.D. Velleman, The Genesis of Shame, 30 Philosophy and Public Affairs 27-52 (2001).

Virgil v. Sports Illustrated, 527 F.2d 1122, 1128 (9th Cir. 1975).

Virgil v. Sports Illustrated, 424 F. Supp. 1286 (S.D. 1976).

"Wikipedia:Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

"Why is My Court Case on the Internet?" Public.Resource.Org, https://public.resource.org/court_cases.html.

"You Are What Google Says You Are," Wired. Feb. 11, 2009.

Zogby International Poll, http://www.ftc.gov/os/comments/privacyreportframework/00457-57996.pdf (2010).

Juliet Lodge:

The promise of ethical secrecy: can curiosity overcome automated group-think?

Abstract:

Secrecy and transparency are fundamentally undermined by automated decisionmaking that transforms our understanding of where we begin and end, of self and society. This article considers whether and how technological applications compromise secrecy, transform our perception of the idea appropriate disclosure, our interaction in society and the society itself. It argues that secrecy is part of a continuum of transparency and accountability that cannot be reliably sustained and mediated by automated decisionmaking devoid of curiosity. Do we need an ethics of secrecy derived, perhaps, from our understanding of harmful effects of disclosure?

Agenda

Author:

Prof. Dr. Dr Juliet Lodge

- Jean Monnet European Centre of Excellence, University of Leeds, LS2 9JT,UK.
- ✉ j.e.lodge@leeds.ac.uk

- Relevant publications:
  - (2011) 'Transformative biometrics and the exercise of arbitrary power', in A.Bromme, C.Busch(Eds) Biosig. Fraunhofer Institute. Darmstadt, Gesellschaft fur Informatik.67-78.
  - (2010) Quantum Surveillance and shared secrets: a Biometric step too far? CEPS, Brussels, 2010
  - Biometrics in the EU, Report for the LIBE committee of the European Parliament, Brussels, 2010.

ISSN 1614-1687

'We are neither a society of angels nor one of devils, neither a fully open society nor a secret one. This is the reason why the difference between public and private as well as between public and secret is so relevant for every human society'[1]

1 Where do I begin?

As every parent knows, part of a baby's development is about the exploration of the limits of the physical self. As a baby plays with his toes, he discovers limits: where do I begin and end? As he moves on to engage in and arguably depend on an ICT enabled world, the binary self-other distinction that provides content for conceptions of internal and external, private and public, subject and object becomes increasingly murky. Machines, even RFID - or nano therapeutic medical - implants, condition his behaviour, sometimes imperceptibly and without him consciously noting as much. Sometimes overtly, in denying or facilitating access to space, goods and services, as in the case of automated border controls.

This rather mundane example of denial of access, however, highlights a tension in our understanding of identity, how we identify ourselves in private and in public and how that is captured by machines that have the capacity to intrude on and dissolve the border between the self and other, the internal and external, the private and public. This gives rise to anxiety over personal space and privacy. It also leads to a disingenuous countervailing rhetoric on 'open government' which has little to do with transparency and accountability, and much to do with the processes that lend themselves to being depicted or enacted by computer code. Putting government or public authority information (such as civil registration documents, committee meetings, government structures and so on) online does not equate to openness. Pictograms and dates are useful and essential for *response, reflection and external input.* These merely suggest that such domestic civil procedures are not hidden: secrecy is not the dominant norm.

Contrast that with: personal online activity, whether in social media or accessing of services; corporate online behavioural tracking; malevolent intrusion, and e-crime. There, invisibility and in effect 'secrecy' to facilitate evasion from immediate detection for whatever reason, are common. Here the personal and the private become commodified and re-configurable (with or without the individual person's explicit knowledge or consent). In that case, something occurs 'in secret', possibly to their detriment and certainly in a way that in some measure exploits and capitalises on them. Is it possible to identify and define ethical secrecy?

1.1 Lies, damned lies and secrets

Secrecy has become a dirty word in politics. Secrecy is suspect. But it is not the antithesis of transparency. A more nuanced appreciation is necessary. Without curiosity, neither secrecy, openness, transparency and accountability are credible.

Secrecy is necessary to operational effectiveness in the administration of certain (normally extra-border, external) parts of public policy. Secrecy is intrinsic to our daily lives, not because we have something (shameful) to conceal but because we have something we choose not to reveal, or see as inappropriate to disclose in specific situations. This neither makes us suspect nor does it mean that secrecy and transparency are not part of a continuum of private and public life. Appropriate disclosure helps ensure civility. If everything is potentially open to being disclosed, with or without the subject's knowledge let alone informed consent, is secrecy robbed of meaning? How is our world and society transformed? Are there some conditions under which silence should imply not consent (as in the Anglo-saxon world) but intentional secrecy? Do we need an ethics of secrecy derived, perhaps, from our understanding of harmful effects of disclosure? The ethics of secrecy requires us to consider under what conditions secrecy has been justified.

[1] Capurro, Never enter your real data. 75.

1.2 Secrecy as a justifying rationale

Secrecy is a term traditionally associated with ensuring security. In western, liberal democratic tradition, secrecy has been put forward as the legitimate and justifiable exception to the rule of openness and transparency in order to safeguard a state's security and liberty. Security and liberty are part of the same continuum. However, the state's ability to sustain and enforce secrecy in the name of security and liberty has been eroded by many factors, including:

- technological innovation and new applications especially for mobile telephony
- robotisation and automation of processes previously requiring a human to exercise judgement and make an informed decision on the next step through the use of 'smart borders', RFIDs, nano-sensors, robots, ambient intelligent environments
- multi-use technologies, such as brain imaging and therapeutic interventions, for 'security' purposes
- public private partnerships and semi-privatisation in administering public government services (in-cluding aspects of security and policing)
- out-sourcing data and information storage, destruction and analysis beyond the borders of the state, including the cloud
- securitizing domestic politics (including leisure, education, health, civil document based data by re-quiring data retention for 'security' purposes)
- allowing data provided for one purpose to be re-used or reconfigured for imprecise purposes by un-known 'others' in the name of transparency broadly conceived and in order to maximize the value of open data
- automated cross-border information exchange[2]

Technological innovations and new applications have eroded the boundaries between the public and private world to the extent that their almost imperceptible, yet accelerating, merging makes it difficult to identify and relate to the traditional structures and norms of accountable actions. Critical infrastructure attacks, denial of service attacks, malware and intrusion can be conducted from outside the jurisdiction of the government or organisation that commissioned the programme running them. How, in such an instance, is government or the appropriate authority to be held to account? Legal liability to gain financial redress is too often paraded as the appropriate response when in practice it is merely a symbolic response. Claiming to exert control via ACTA, too, may prove chimerical by facilitating the very intrusive tracking by invisible machines/ISPs on private/secret activity that the ordinary person abhors. Informational self-determination is a laudable ideal, informed by ethical principles of tolerance, openness, purpose specification and informed consent. It is far from universally accessible, let alone – currently – operationally or technically absolutely possible.

The traditional idea of a visible face being linked to responsibility for performance is undermined by new technological applications. Who or what can we trust as reliable and under what circumstances is that trust warranted?

The same applies in the private realm. While some people lead imaginary second lives as fantasy avatars, others transform their cyber criminal exploits into tangible actions traceable and apprehendable by cyber police. The anonymous avatar is not technically synonymous always with a 'secret life'.

Identities and means of proving and claiming an identity that we thought we could rely on and trust (such as birth certificate, civil registration documents and passports) are only as reliable as the enrolment procedures for ensuring the authenticity of the original. Fingerprinting babies at birth and deriving a biometric 'breeder identity document' from that is not foolproof[3]. Moreover, false or poor quality breeder documents can multiply problems for genuine individuals long into the future. Yet, those agencies, ICTs or codes that

[2] Lodge,73.

[3] http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports

generate them remain largely invisible or at least able to blame errors on 'computer code' without, at present, the public being apprised of the relative reliability and trustworthiness of the ICTs used. Commercially sensitive or politically, security sensitive information (however that is defined) continue to rely on the legitimating rationale of secrecy. However, if this can and is increasingly breached, should everything be in the public domain with a free-for-all or should there be an ethics of secrecy or practice that is informed by ethical secrecy?

2 Openness the antidote to secrecy to reconnect governments with citizens

To some extent governments have recognised that in invoking 'secrecy' rationales to legitimate their securitization of domestic politics requires a counter-weight. Accordingly, the rhetoric of 'reconnecting' with citizens through ICTs has been used to counter the charge of excessive securitization of domestic politics and the private realm by public authorities. This has not been adequately demonstrated in the case of public-private partnerships.

Among the attractions of ICTs for governments has been the illusion they have offered of making government appear more transparent and less secretive to citizens by reconnecting rulers and the ruled through, for example, 'open government', e-voting, online petitions and blogs. ICTs offer the mirage of facilitating benevolent reconnection of citizens both with each other in an e-public sphere and with political contestation, without offering the democratic counterweight of protection against the abuse of power. Instead, technical fixes and data protection laws have been advocated. These include, baked in security by design to make data privacy a first principle rather than an after-thought in the design of systems and applications.

But the preoccupation with privacy, its commodification and privatization, risks compromising our understanding of secrecy and the situations in which secrecy is a precondition of operationally safeguarding security and liberty, and an imperative for sustaining visible, public democratic accountability of those who administer processes and control access to them.

Governments have ceased to be the single, authoritative locus of authority or enabler of access to public services and protector of citizens' and territorial security. In a modern hyper-connected world, access or use of e-services is not simply a matter of digital literacy. The well-known inhibitors such as age, physical or mental incapacity, digital illiteracy, or poverty are dwarfed by technical applications that allow invisible agents to intrude, to deny access to services, to censor, or to cyber-attack critical infrastructures as well as individual people. The cloak of invisibility around malevolent cyber-attacks exacerbates the vulnerability of all: governments, corporations, citizens.

Whom to trust to safeguard security then becomes an interesting question. More interesting still, perhaps, is the question of whether informational secrecy in the public domain is a threat to individual and collective security? Should it be kept purely for our most personal private lives, even though that is technically impossible?

Is privacy itself so technically suspect and emptied of meaning that it is irrelevant to individual security and secrecy? Is the protection of an individual's ICT enabled identity token a necessary aspect of protecting that person's safety and security, or collective safety and security? Should such identity tokens be secretised? By whom, under what circumstances? For how long? Should secrecy be commodified? Is it realistic to expect government to protect state and personal secrecy? If governments were able to do so, would public trust in the credibility of government authority be restored? Can ethical secrecy be sustained by traditional, liberal democratic government structures and practices or does technological innovation and particularly automated, cross-border information exchange, constrain, dissolve or facilitate it?

2.1 ICTs and sustainable democratic accountability

As public administration is externalized, outsourced or shared in private-public ICT partnerships, the political master is replaced by a commo-techno (commercial-technological motor) that eludes public control, except possibly through the purse. The managerialist approach to ICT 'good practice' relies on voluntary, ad hoc and imperfect compliance. A quick fix to claiming transparent accountability, it veils the semi-privatisation of political accountability and differential security in opaque terms not susceptible to public, external scrutiny.

Data Protection and privacy commissioners and laws cannot effect sufficient politico-legal control. They are necessary when people with official documents that authenticate them (something not universal yet) are trackable by computer code. They are insufficient for protecting and allowing the data subject to discover and revise data held about him, and for allowing consistent and coherent access to data for use in criminal investigation for those responsible for investigations. This is not just a matter of relative forensic capabilities, data retention practices and ICT legacy systems, contrary to what the recent EU Commission Communication (2012) suggests). The blurring of responsibilities regarding e-information means that both public and private authorities tend to gloss over problems of accountability, or contest responsibility and/or capacity to pay when facing big fines. A British public health trust raised ethical questions when the British Information Commissioner's Office levied the largest ever fine following the sale in internet auctions of some of its de-funct hard drives containing sensitive personal data by the IT provider. The trust suggested that the fine was disproportionate to its duty to provide health care in times of recession[4]. Should there be a hierarchy of ethics to reflect the relative value attaching to differential privacy, secrecy and implementing practices in public-private partnerships. e-commodification of personal information in fuzzy e-space is insufficiently susceptible to visible, authoritative public regulation and accountability. For constitutionalists, the assumed bargain between the state and citizen, aggravated by legal uncertainty, will be broken no matter how ubiqui-tous 'surveillance' in its many guises. Security is no longer simply a matter of safeguarding territorial integri-ty. ICTs' ubiquitous impact on citizens' lives and geo-cyber attacks on critical infrastructures are not amena-ble to the traditional defences offered by international treaties. Electronic networks link public and private organisations in ways that so far escape effective technical and political oversight and control. Is a tragedy of the increasingly re-bordered domestic and internationalised cyber-spaces of the ICT commons is inevita-ble?

3 Inverting the secrecy bargain

Transparency and accountability are essential to prevent an abuse of power and vital to allowing parliament to hold government in check. In fields traditionally subject to the security exceptionalism associated with secrecy rules and intelligence, questions arise over an assumed proper balance between the requirements of liberty and of security. While perfect equilibrium is unrealistic, creeping exceptionalism undermines sustain-able liberty. If legitimacy is challenged by the people or worse still by invisible cyber-attacks, what are the prospects for the democratic exercise and locus of justice, authority and power? In such a scenario, does secrecy endanger security?

Absolute openness and absolute secrecy? What are the disruptive consequences of secrecy? Of refusing to share information in formerly trusted groups? Does dishonesty become the shield against breaches of secre-cy, so that no one is ever (quite) who they say they are? While absolute secrecy is neither possible nor desirable, an element of secrecy is necessary to trust. Moreover, the artificial duality of absolute secrecy versus absolute openness is misleading because it misses the point of the necessity of the intervening varia-ble of curiosity.

[4] Information Commissioner's Office (ICO). In June 2012, Brighton and Sussex University Hospitals NHS Trust was issued with a Civil Monetary Penalty (CMP) of £325,000 following a serious breach of the Data Protection Act in 2010. The ICO was granted the power to issue CMPs in April 2010.

4 Conclusion: Curiosity: the intervening variable

Without curiosity, secrecy is arguably not necessary. Without curiosity accountability becomes no more than a mechanical action, a knee-jerk reaction. Without curiosity, the disclosure and non-disclosure of information lacks purpose : the right to know and the right to be forgotten are mired in an expectation that someone or something somewhere is sufficiently curious to want to know or to forget and erase.

What is problematic about secrecy and ICTs is the possibility that (non) disclosure may cease to depend on human decision; that they may not be conditioned by precautionary considerations of whether or not exceptional circumstances justify the release of information without prior consent in order to prevent harm. Disclosure is not only part of the discourse of secrecy versus openess but also of individual and collective harm versus an evaluation of less intrusive/more conditional considerations regarding when, how and to whom disclosure should be made or secrecy preserved.

Once this decision is automated and becomes a mechanistic reflex where judgement associated with curiosity and reflection are absent, the potential transformative impact on society is extensive. Machines, computer code or robots that automatically disclose or withhold information do not necessarily refer to explicit moral values before doing so: those of the original, invisible and unaccountable programmer(s) determine what technical process is enabled. It is easy then to reflect on the duties of machines vis-a-vis humans without first considering what level and scope of data sharing, disclosure of secrecy might be contingent or legitimate in given circumstances.

Since machines are able to select and make linkages between data fields, and 'learn from other machines', group think is inevitably entrenched in how we conduct our lives. Is that group think potentially more dangerous than that experienced in policymaking circles in history? By reconsidering secrecy, could scientific innovation help to restore confidence and trust in our ability to strive for the common good through an ethical use of ICTs?

It is disingenuous to suppose that it would be safe to rely on machine-led disclosure and secrecy. What are the implications of attacks on hyper-connectedness? Here we are not concerned with IPR, duties of care, legal and financial redress. We are concerned with the ethical impact on society, how humans conduct their lives, human self-understanding, ICT substitution for realtime human reasoning, the technisation of the self, techno-dependency, the implications of the erosion of stable interfaces between man and ICTs, and the evolving digital values to sustain civilised society. We are concerned with how ideas of sufficient privacy and sufficient secrecy are being reconfigured as anonymisation codes of practice implying the elaboration of a hierarchy of ethical secrecy.

References

*Capurro, Rafael (2011)**:** Never enter your real data, IRIE,vol 16, 74-8.*

Council of the European Union (2011) Commission Services Communication to the Working Party on Data Protection and Exchange of Information, Consultation on reform of Data Retention Directive: emerging themes and next steps, Doc 18620/11, Brussels, 15 December.

Information Commissioner (ICO) (2012) NHS Trust fined £325,000 following data breach affecting thousands of patients and staff. Press release. http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx.

Lodge, J (2009) Transparency and Accountability: from structuro-procedural transparency and institutional accountability to communicating (in)security in digi-space in (D.Bigo ed) Europe's 21st Century Challenge: Delivering Liberty and Security.Ashgate

Edward H. Spence:

Government Secrecy, the Ethics of Wikileaks, and the Fifth Estate

Abstract

This paper aims to systematically explore and provide answers to the following key questions: When is government secrecy justified? In a conflict between government secrecy and the public's right to be informed on matters of public interest, which ought to take priority? Is Julian Assange a journalist and what justifies his role as a journalist? Even if Julian Assange is a journalist of the new media, was he justified in disseminating classified information to the public? Who decides what is in "the public interest"? Is it only journalists of the Fourth Estate who decide that or also journalists of the Fifth Estate (new media)? This paper will answer the aforementioned questions by arguing that the media in the form of both the Fourth and Fifth Estates should inform the public on matters of public interest truthfully and ethically, even if sometimes they have to breach government secrecy.

Author:

Author:

Edward Howlett Spence

- BA (Hons, 1st Class) PhD (University of Sydney)
- Senior Lecturer (Philosophy and Ethics), School of Communication and Creative Industries
- Senior Research Fellow, Centre for Applied Philosophy and Public Ethics (CAPPE)
- Research Fellow, 3TU. Centre for Ethics and Technology, Den Haag, Netherlands
  http://www.ethicsandtechnology.eu/people/spence_edward/
- Charles Sturt University, Panorama Avenue, Bathurst, NSW 2795, Australia
- ☎ +61 2 6338 4520

1 Introduction

In disseminating classified information to the public, Wikileaks and its founder Julian Assange stand accused by an assembly of world politicians for doing something terribly wrong. Yet upon further reflection and all available evidence so far, this is by no means obvious. One could argue that on the contrary, in his capacity as a social journalist, if that is what he is, Assange could not have done otherwise. In disseminating information of public interest, Assange seems to have done the right thing. He informed the public of the truth. The further question that needs to be examined, however, is if the truth was a state secret of national security was it in the public interest to have kept it a secret instead of publishing it? Is this a case where the public interest would have been best served by withholding information and keeping the relevant classified information a secret?

Australia's Media and Entertainment Arts Alliance (MEAA) journalism code of ethics states that "respect for truth and the public's right to information are fundamental principles of journalism". Similar principles are also enunciated by the code of ethics of the International Federation of Journalists (IFJ), which declares that "respect for truth and for the right of the public to truth is the first duty of the journalist".

According to those national and international journalism codes of ethics, Julian Assange, in his assumed role as a social journalist, has committed no wrong, at least no moral wrong, in disseminating documents concerning diplomatic classified information, if the dissemination of such information was in the public interest. His actions may have breached some as yet unidentified laws but that has yet to be established. However, even if it turns out that he has somehow technically breached some law concerning the dissemination of classified information that in itself does not make his actions ethically wrong. For consider: those courageous people who infringed the now discredited apartheid laws of South Africa did break the law but in doing so acted morally out of a sense of universal justice. Assange may in fact have acted as any honest, vigilant and competent investigative journalist does or ought to do, the world over. Consider for, example, two previous famous cases, those of *Watergate* and the *Pentagon Papers*. In both those cases, journalists disseminated information to the public that the US government at the time wanted kept secret. As it turned out, however, the information although embarrassing and damaging to the government was in the public interest.

As in the aforementioned cases, whether or not the information disseminated by Wikileaks was in the public interest may be a matter for the public to decide and not politicians who would rather keep their citizens in the dark and ignorant on some vague and misguided notion that they do so for the good of their citizens. Plato may have argued for the "noble lie" in the *Republic* when it serves the public interest, but there is nothing noble about lying or lying by omission in hiding and keeping secret, politically inconvenient truths.

Politicians serve the public interest and not the other way round. It is indeed this sentiment that gave rise to the perception of the media as the Fourth Estate. An independent and fearless disseminator of true information to the public so that citizens are able to make informed decisions on matters of public interest, which contribute to the common good and serve democracy. The advent of the Internet and other information and communication technologies (ICTs) such as smart phones and twitter has enabled anyone to source and disseminate information of one-to-many, many-to-many, and many-to-one, anywhere, anyway, at any time. I will argue in this paper that the Internet and its associated ICTs have ushered in the *Fifth Estate*, endowing every citizen with the potential and opportunity to be a journalist. If this is correct, then Assange qualifies as a journalist of the Fifth Estate.

Some in the USA, including politicians, have been calling for Assange's blood. Other less bloodthirsty, have been calling for his arrest and indictment. This should not surprise us. After all there is a famous historical precedent for this. Socrates, probably the best known and celebrated philosopher of all times, had to endure as much and worse when he earned the wrath of a few very well-connected and powerful Athenians in 5th century Greece. He was tried and executed on charges for "corrupting the youth and being irreverent to the gods". Though not officially a journalist, he was by his own admission an annoying gadfly tirelessly exposing the ignorance and folly of powerful generals and politicians who claimed to know that which they lacked knowledge of. For Socrates, like committed investigative journalists today, was passionate about the truth. If he had lived today he would probably have been an investigative journalist or a social media blogger in pursuit of the truth for the common good.

Assange of course is no Socrates but if his motives for leaking information to the public are similar to those of Socrates, that is, to inform his fellow-world -citizens of the truth for the common good, annoying or embarrassing as that might be to some, should he not like Socrates as well as the leakers and journalists involved in the Watergate and Pentagon Papers, deserve praise rather than condemnation?

The above introduction was by way of situating and contextualising the following discussion in this paper within the ongoing current debate concerning the rights and wrongs of leaking and publishing classified information that governments wish to keep secret from their citizens.

In addressing the topic stated in the title, this paper aims to systematically explore the following key questions:

1. When, if ever, is government secrecy justified?

2. In a conflict between government secrecy and the public's right to be informed on matters of public interest, which ought to be given priority?

3. Is Julian Assange a journalist and if so what justifies his role as a journalist?

4. Even if Julian Assange can be considered a journalist, at least a journalist of the new media, was he justified in disseminating classified information to the public?

5. Who decides what is in "the public interest"? If it is the media on behalf of the public, is it only journalists of the Fourth Estate (old corporate media) who decide that or also journalists of the Fifth Estate (new media)?

6. Do we trust the media to make that decision on our behalf?

In summary, this paper will answer the aforementioned questions by arguing that the media in the form of both the Fourth and Fifth Estates should inform the public on matters of public interest truthfully and ethically, even if sometimes they have to breach government secrecy. However, in order to do so, it is essential that the media is trustworthy and credible. Insofar as the government is the elected representative of the public, it is accountable to the public. Insofar as the media's role is to inform the public on matters of public interest, the media must be trustworthy to fulfil that role without fear or bias, even if it means having to sometimes breach government secrets. After all, the primary role of the media in a democracy is to keep the government accountable. To do so, the government must be transparent, and it is the role of the media to provide transparency on matters of public interest. However, a key question this paper will address is whether in the wake of the *News of the World* phone-hacking scandal the media can be trusted to fulfil that role. Is the media, especially the corporate old media, as untrustworthy as the government in engaging in covert operations that harm rather than benefit the public for their own self-regarding interests?

2 Government secrecy: when is it justified?

Sissela Bok in her book (1982) *Secrets: On the Ethics of Concealment and Revelation*, defines "secrecy" as "intentional concealment" and "privacy" as "the condition of being protected from unwanted access by others – physical access, personal information, or attention" 1984: 10-11). Although sometimes the two overlap, when each involves concealment, secrecy and privacy, however, are different since what is private need not involve secrecy. For a private life, as Boc correctly points-out need not be and very rarely is a secret life (1984:11). Unless directly relevant to our discussion, this paper will only be concerned with secrecy, and government secrecy in particular, and not with privacy.

The question I shall be addressing in this section is what, if anything, justifies government secrecy. The related question whether government secrecy even when justified can be overridden by other conflicting considerations, such as the public's right to information, will be taken up in section (3).

"Reason of state" is one of the best known rationales offered for justifying government secrecy. The idea being that certain actions that would be deemed immoral if performed by individuals are justified when performed by the state. The usual justification offered is that individuals could not survive without the state. So when necessary for its survival and by extension the survival of its individual citizens, the state is justified in engaging in actions, which would otherwise be deemed immoral, including secret actions involving lying, cheating and in some cases torture, and murder (Boc 1984: 173).

A justification of this kind based on "reason of state", whether sound or not, could conceivably be offered for the existence and secret operations of the US Army detention camp at Guantanamo Bay. However, an argument against secrets of state is Bentham's claim that "secrecy, being an instrument of conspiracy, ought never to be the system of a regular government", which according to Boc is echoed also by Woodrow Wilson's observation that "government ought to be all outside and no inside" and that "there ought to be no place where anything can be done that everybody does not know about" (Boc 1984: 171).

Lord Acton makes a similar claim to the effect that "everything secret degenerates, even the administration of justice; nothing is safe that does not show how it can bear discussion and publicity" (Boc 1984: 105). The appeal to publicity is also reflected in Kant's legitimacy test of publicity. According to Simone Chambers, Kant claims that "all actions affecting the rights of other human beings are wrong if their maxim is not compatible with their being made public" (Chambers 2004: 406). The appeal to publicity provides a powerful prima facie reason against government secrecy, especially when that secrecy combined with power, can be used, and often is used, to violate human rights.

However, Chambers argues correctly that some government administrative secrecy is necessary for rational and critical deliberation on matters of policy. He offers that "deliberative secrecy" is justifiable as a "way of encouraging better discussion and fuller consideration of legislation" (Chambers 2044: 394) if such deliberative secrecy meets the "deliberative secrecy test", namely, "a secret or set of secrets is not justified merely if it promotes deliberation on the merits of public policy; citizens and their accountable representatives must also be able to deliberate about whether it does so". Chambers refers to this test as "a form of retrospective accountability for the process as well as for its results" (Chambers 2004: 394).

According to Chambers, ideally deliberative secrecy should meet two conditions of "public reason": (a) the justification test of "Socratic reason" that requires justification for one's beliefs and claims based on sound arguments that other reasonable people at large could accept and (b) the democratic accountability test that requires public legitimacy, through the democratic process. In a nice formulation of public reason, Chambers states that "the Socratic element stresses the rationality of public *reason* while the democratic element stresses the pubic nature of *public* reason" (Chambers 2044: 391).

However, quite correctly Chambers also recognises the potential conflict or at least tension that can arise between the two. For Socratic dialectic based on rational arguments of justification favours primarily the *rational* aspect of public reason, whilst rhetoric based on persuasion favours primarily the *publicity* aspect of public reason. Since persuasion as the effectiveness of advertising and propaganda demonstrate need not be rational or justifiable but merely persuasive or popular, it can undermine the rational aspect of public reason, and sometimes at least in politics, does so.

This brings us back to why sometimes administrative deliberative secrecy in rational political debate on policy issues may be necessary. So long as decisions made in camera can be defended to the public or their representatives on justifiable and rational grounds, some deliberative government secrecy may be unavoidable and indeed desirable. Importantly, however, it must meet both the rationality and accountability conditions of public reason. This, however, may be easier in theory than in practice and the difficulty reflects John Stuart Mill's concern of "how without publicity could citizens either check or encourage what they are not permitted to see" (Boc 1984: 179). For as Boc correctly observes "concealment insulates administrators from criticism and interference; it allow them to correct mistakes and to reverse direction without costly, often embarrassing explanations; and it permits them to cut corners with no questions being asked" (Boc 1984: 177).

When it comes to secrecy on military matters things get even more complicated. Boc observes that "the contradictions and tensions of secrecy are never stronger than in the military stance of nations" (Boc, 1984:191). Even Bentham, according to Boc, who was otherwise against government secrecy, was willing to concede that publicity, one of the corner stones of deliberative democracy, should be suspended if it favoured the enemy (Boc 1984: 194). Against that sentiment, Boc, however, rightfully, cautions that

> *"Under conditions of crisis, when nations feel beleaguered, military secrecy is likely to spread, invite abuse, and undermine the very security it is meant to uphold. The burden of excessive secrecy can be heavy; and the suffering it inflicts, domestically and abroad, may far outweigh even the strict military objectives it was meant to ensure"(Boc 1984: 194).*

The torture, abuse and degradation of prisoners at Abu Ghraib in Iraq illustrate just one of many cautionary cases that can be marshalled in support of Boc's concern of allowing the military too much secrecy. Unchecked military secrecy can lead to moral wrongs. Another more recent case, more focal for this paper, is that of Bradley Manning, the 24-year-old Army intelligence analyst who stands accused of releasing the *Collateral Murder* video as well as other classified documents to Wikileaks. The video that shows unarmed civilians and two Reuters journalists being killed by a US Apache helicopter crew in Iraq, received wide publicity in the mainstream media. It's a paradigmatic example of the symbiotic relationship that now exists between the old corporate media and the new social media. It demonstrates how corporate media increasingly uses content generated by media- activist sources such as Wikileaks and many others to inform the public, and sometimes unwittingly as in the case of the "Gay Girl in Damascus"[5] case misinform the public, on matters deemed to be of public interest.

Another paradigmatic case of making public that which the government and the military wanted kept secret and concealed from any public scrutiny is of course the *Pentagon Papers*. Boc quoting Daniel Ellsberg, the man in the Nixon Administration who leaked the Pentagon Papers story to the media, tells us how Ellsberg expressed the need to "find oneself loyalties long unconsulted, deeper and broader than loyalty to the President: loyalties to America's founding concepts, to our constitutional system, to countrymen, to one's humanity" (Boc 1984: 207). This was the man that Henry Kissinger had declared the "most dangerous man in America". He was of course right. For those who seek the truth and are prepared to go to great lengths and at personal risk to themselves to bring it to light for the public good are often considered "dangerous" by the state.

3 The conflict between the government's right to secrecy and the public's right to know

Whistle-blowers and leakers are traditionally seen as the enemies of state secrets. Acting sometimes by stealth as in Bradley Manning's case or openly as in the case of Daniel Ellsberg they claim to act on moral conscience by undertaking to make public for the common good what the state wants concealed. Manning and Assange more recently and Ellsberg before them leaked information to the public that they considered the public had a right to know. Before we proceed to examine under what conditions whistle-blowers and leakers are justified in publishing classified information to the public the state regards as secret, we must first enquire as to whether or not the public has a right to such information. What justifies such a right, and is such a right robust enough to override in principle, the state's conflicting right to secrecy?

I would like to suggest that Socrates was probably the first investigative journalist. He is also one of the greatest philosophers and as relevant and inspiring today as he was 2500 thousand years ago. According to

[5] The "Gay Girl in Damascus" case refers to an online blog that was supposedly written by a lesbian young woman named Amina Arraf living in Damascus. It purported to give minute by minute reporting on the Syrian conflict. The blog was in fact a hoax that was written by Tom MacMaster, a graduate student from the University of Edinburgh. It attracted wide publicity from around the world and led to its publication by the mainstream international media.

the Oracle of Delphi he was also the wisest. Being accused of "being irreverent to the gods and corrupting the youth of Athens" he told the court at his trial that like a "gadfly" his mission was to engage his fellow-citizens in debate on matters of virtue, truth and wisdom. He was sentenced to death by hemlock for his troubles. In his closing speech to the jurors he reprimands his fellow-citizens for caring more about money and reputation than about morality and knowledge: "O my friend, why do you who are a citizen of the great and mighty and wise city of Athens, care so much about laying up the greatest amount of money and honour and reputation, and so little about wisdom and truth…? Are you not ashamed of this?" (Plato, *Apology*)

Since Socrates, many good and worthy of the name journalists have followed Socrates' footsteps. Some like legendary US journalist Edward R. Murrow who took on Joseph McCarthy and won at a time when all walked in fear of McCarthy; the respected Australian journalist Chris Masters who exposed wholesale police corruption in Queensland in the 1980s, and two women journalists, the Irish Veronica Guerin and the Russian Anna Politkovskaya, who like Socrates paid with their lives for informing the public of what they thought the public had a right to know. These journalists, whether consciously or not, shared Socrates' unshakeable conviction that truth and knowledge is the bloodline of a free democracy. And for present-day deliberative democracy the dissemination of information to the public on matters of public interest is arguably essential. This provides some initial justification for the claim that the public has a right to know of what the government gets up to. They have that right in view of the fact that citizens form part of the democratic process and therefore must have the necessary information to enable them to participate, at least in principle if not always in practice, in the deliberations carried out on *their behalf* by their elected representatives.

That conviction is also expressed in Australia's *Media and Entertainment Arts Alliance* (MEAA) journalism code of ethics, which states that "respect for truth and the public's right to information are fundamental principles of journalism". Similar principles are also enunciated by the code of ethics of the International Federation of Journalists (IFJ), which declares that "respect for truth and for the right of the public to truth is the first duty of the journalist". The *News of the World* phone-hacking scandal by extreme contrast has shown us that very bad things can happen when journalists turn from seeking truth to engaging secretly in crime and corruption, putting profit before propriety.

In a previous publication (Spence 2003) I presented an argument for the justification of the claim that the public has a right to information. Due to constraints of space I reproduce the argument here only in summary:

The public has a right to information on matters of public interest such as health, education, war and government, among others, because it is in their interest to have that information. Why is it in the public interest to have such information? Before we can answer that question we must first define "public interest". I have proposed the following general definition: "public interest" is whatever secures and promotes the public's individual and collective rights to freedom and wellbeing.

Using the above definition we can now say that it is in the public interest to have access to information because such information can help secure and promote the public's collective rights to freedom and wellbeing. To the extent that the public requires information to secure and promote their rights to freedom and wellbeing, both individually and collectively, it is in the public interest to have such information. Informing the public about political, police, and corporate corruption, as in the current ongoing case of the *News of the World* phone-hacking scandal, are just some examples of how media information is in the public interest. It is in the public interest just because it helps secure and promote the public's rights to freedom and wellbeing.

As to the further question of why the public has rights to freedom and wellbeing my answer, which I cannot offer here in detail as it goes beyond the scope of the specific aims of this paper, relies on a further argument based on Alan Gewirth's Principle of Generic Consistency (PGC). Briefly, the argument is that the public has rights to freedom and wellbeing because the public comprises of particular purposive agents who individually and collectively have rights to their freedom and wellbeing in accordance with the Principle of Ge-

neric Consistency (PGC)[6]. In conclusion, insofar as the public needs information to be able to make informed decisions on matters of public interest that affect both individually and collectively their rights to freedom and wellbeing, the public has a right to receive information from the media because it helps secure and promote those rights.

Having established that the public has a right to information we can now examine under what conditions and circumstances whistle-blowers and leakers are justified in publishing or arranging the publication of classified information to the public that the state regards as secret. Boc identifies three elements that characterise the dissemination of secret information to the public by whistle-blowers or leakers (for ease of reference I will henceforth use the term "leakers" to apply to both) and which together appear to provide prima facie justification for that practice.

The three elements are those of *dissent*, *breach of loyalty* and *accusation*. In addition, the accusation element concerns a present or imminent threat (Boc 1984, 214-215). In the case of leaking, dissent according to Boc involves disagreement with authority and more specifically it involves exposing negligence or abuse, alerting the public to a risk and assigning responsibility for that risk (Boc 1984: 214). Leaking also involves a breach of loyalty as it comes from an inside source. This typically places the leaker in a conflict of two loyalties, first, to their organisation and second, to the public. Thus Bradley Manning may have faced this conflict when leaking classified information of the US military to the public via Wikileaks. Leaking is also characterised by accusation, as it is intended as chastisement towards those within the leaker's organisation involved in unethical and/or illegal conduct. And finally, according to Boc, leaking concerns present or imminent threat (Boc 1984: 215). In the case of Bradley Manning although the leak concerned past events, such as the *Collateral Murder* video, the general threat that he perceived may have been the ongoing and systematic ethical abuses conducted by the US military in Iraq and Afghanistan.

Both Bradley Manning's and Daniel Ellsberg's leaking of information, the former secretly, the latter openly, illustrate the three characteristics of the practice of leaking identified by Boc. In addition, as Boc correctly observes, the three elements of dissent, breach of loyalty and accusation, also characterise the moral choice that leakers typically face. The correct choice is to leak information to the public when such information is considered essential and vital for the public good. In view of the moral weight and seriousness of the information leaked by Manning and Ellsberg respectively, such information can be seen to qualify as a matter of public interest. Hence, that information also qualifies as information to which the public has a right, since it potentially impacts on the public's individual and collective rights to freedom and wellbeing, as argued above; both narrowly in the case of US citizens who have a right to know what their government and their military does or does not do on their behalf, and more widely, in the case of non-citizens whose human rights were abused by the alleged violations contained in those leaks.

4 Are new media activists the new journalists of the 5th Estate?

In his article "Who is a Journalist" (Black 2010) Jay Black explores the question of who is a journalist? According to Black "broad-based citizen and web-based journalism augments the knowledge base and is making a persuasive case for enjoyment of the status, rights, and protections formerly enjoyed only by the elite media". "Now" as he correctly points out, "is not the time to argue for a narrow definition of journalism" (Black 2010, 112). He concludes that "the issue of who is a journalist should not centre on where one works, but on how one works" (Black, 2010: 114). Black's wider definition of who is a journalist, highlights correctly a major issue of journalism ethics raised by Christopher Meyers in the introduction to his edited book (Meyers, 2010) namely, that epistemic credence and trust is at the centre of who and what a journalist is or at least ought to be in principle – not just in name and style but more fundamentally and crucially, in substance. I agree with both Black's wide definition of what constitutes a journalist as well as with Myers' claim above concerning epistemic credence and trust. For what matters with regard to the dissemination of information both in the case where the dissemination is by a professional journalist of a major newspaper,

[6] For further details for the justification of the argument for rights to freedom and wellbeing, based on Alan Gewirth's Principle of Generic Consistency see Spence 2006, *Ethics Within Reason*.

such as the *UK Guardian*, for example, or by a "web-based journalist" or "citizen journalist" writing a blog on the Internet, is whether the information is credible and reliable with regard to truth and trust, especially on matter of public interest.

Insofar as Julian Assange, has been disseminating information on his Wikileaks website that is true, credible, reliable, and trustworthy, and moreover, information that is of public interest , he too can, as he himself claims of himself, be considered a journalist, a journalist of the 5th Estate. I define the 5th Estate loosely here as the Estate comprising all the world-denizens operating in cyberspace that as individuals or groups disseminate information on matters of public interest to the world at large. And do so without fear or favor. In this regard, they provide an invaluable service in the best tradition of investigative journalism but without the commercial constraints that unfortunately sometimes at least undermine, restrict or even muzzle good investigative journalism, or worse, lead to the kind of gross ethical and legal abuses evident in the News Corporations, *News of the World* phone-hacking case.

Increasingly, as already mentioned, a symbiotic relationship is fast developing between the journalists of the 4th and 5th Estates. When done correctly, as in the case of the information leaked by Bradley Manning on the *Collateral Murder* video and publicized by Wikileaks and later the mainstream media that symbiotic relationship augments the quality and quantity of information disseminated to the public on matters of public interest and enhances the substance and scope of deliberative democracy. However, when done wrongly as in the case of the *Gay Girl in Damascus* blog, information becomes misinformation or worse, disinformation that undermines the public interest and casts doubt on what one can accept as true or dismiss as false on the Internet. This is a major challenge both for the journalists of the 4th and 5th Estates. Ultimately it comes down to a question of trust, a much larger issue which lies beyond the scope of our present discussion.

Lee Wilkins correctly argues that in addition to their traditional role of informing the public, journalists should also seek to mitigate harm to the public. To do so, she says, the definition of news should not only include what actually happens but also what might happen. As Wilkins eloquently puts it "preventing harm becomes the predominant ethical obligation" of journalists (2010, 313). Journalists, she argues, should become "mitigation watchdogs". Wilkins' argument for "mitigation reporting" sits well with my own position that a global ethics requires not only a negative duty of not causing harm but also a positive duty of offering others positive assistance and promoting their welfare when we can (Spence, 2007).

In agreement with Wilkins, this should include journalists acting as "mitigation watchdogs". Wilkins argument lends further value and justification to the role that leakers and whistle-blowers, such as Bradley Manning and Daniel Ellsberg play in the world-wide dissemination of information to the public, with the generous and helping hand of journalists of the 4th and 5th Estates; as in the binary symbiotic relationship between the 4th Estate and Daniel Ellsberg; and equally as valuable and important, the tripartite symbiotic relationship between the 5th Estate in the form of Julian Assange and Wikileaks, Bradley Manning, as well as the 4th Estate, in the form of the international mainstream media that published the leaked information.

The only thing we have to fear from information is that its concealment by governments and the military can lead to far greater harm than its publicity. Specifically, when the information concealed is in the public interest and for the interest of supporting and promoting a healthy and robust deliberative and participatory democracy.

5 Conclusion

This paper has examined what secrecy is and when it is justified in its use by governments. Basing my argument on Sissela Boc's definition of secrecy as "intentional concealment" and Simone Chambers' notion of "deliberative secrecy", I have argued that some government secrecy is justified for rational and critical deliberation on matters of government policy. According to Chambers "deliberative secrecy" is justifiable as a "way of encouraging better discussion and fuller consideration of legislation" (Chambers 2044: 394). Moreover, deliberative secrecy must meet two conditions of public reason: (a) the justification test of "Socratic reason" that requires justification for one's beliefs and claims based on sound arguments that other reason-

able people at large could accept and (b) the democratic accountability test that requires public legitimacy, through the democratic process.

The paper then critically examined the conflict that arises between the government's right to secrecy and the public's right to know. In the discussion of that conflict in section (3), I argued that insofar as whistle-blowers and leakers such as Bradley Manning and Daniel Ellsberg serve the common good in disseminating secret information that is of public interest, they are justified in leaking such information. For it might otherwise not come to light, potentially undermining the principles of deliberative democracy. I then went to argue for the close and symbiotic relationship between journalists of the 4th Estate and those web-based journalists of the 5th Estate, including media-activists and social journalists such as Julian Assange. I concluded that what counts as a journalist in the age heralded as the age of information, is not as Jay Black clams, where one works but how one works. What should guide the journalists of both the 4th and 5th Estates in the 21st century and beyond are the principles of truth, trust, reliability, and justice. The information they disseminate on matters of public interest should be for the public good. To that end, journalists of the information age must not only seek after truth but also after wisdom. For if wisdom is understood as the knowledge of what a good life is and how to live such a life, then surely that is also in the public interest - a public interest that journalists of both the 4th and 5th Estates should promote. Journalists should not only become "mitigation watchdogs", they should also become "wise watchdogs"7.

References

Black, J. (2010) "Who Is a Journalist?" in Christopher Meyer (Ed.) Journalism ethics: A philosophical approach. New York: Oxford University Press, 103-116.

Boc, S. (1984) Secrets: On the Ethics of Concealment and Revelation. Oxford: Oxford University Press.

Chambers, S. (2004) Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation, The Journal of Political Philosophy, Volume 12, Number 4, 389-410.

Meyer, C. (Ed.) Journalism ethics: A philosophical approach. New York: Oxford University Press.

Plato, The Apology. http://classics.mit.edu/Plato/apology.html. Accessed 16 May, 2012.

Spence, E. (2003) Media Ethics: An Ethical Rationalist Approach. Melbourne: Australian Journal of Professional and Applied Ethics Vol. 5, No. 1, June 2003, pp. 35-44.

Spence, E. Ethics Within Reason: A Neo-Gewithian Approach (2006). Maryland: Lexington Books (a division of Rowman and Littlefield, USA).

Spence, E. (2007). Positive rights and the cosmopolitan community: A right-centered foundation for global ethics. Journal of Global Ethics, 3(2), 179–200.

Spence, E. (2011) Information, Knowledge and Wisdom: Groundwork for the Normative Evaluation of Digital Information and Its Relation to the Good Life, Ethics and Information Technology, Volume 13, Number, 3, Pages 261-275.

Wilkins, L. (2010) Mitigation Watchdogs: The Ethical Foundation for a Journalist's Role. In Christopher Meyer (Ed.) Journalism ethics: A philosophical approach. New York: Oxford University Press, 311-324.

[7] For a relevant discussion on information, knowledge, and wisdom see Spence (2011).

Kenneth C. Werbin:

Auto-biography: On the Immanent Commodification of Personal Information

Abstract:

In the last years, a series of automated self-representational social media sites have emerged that shed light on the information ethics associated with participation in Web 2.0. Sites like Zoominfo.com, Pipl.com, 123People.com and Yasni.com not only continually mine and aggregate personal information and biographic data from the (deep) web and beyond to automatically represent the lives of people, but they also engage algorithmic networking logics to represent connections between them; capturing not only who people are, but whom they are connected to. Indeed, these processes of 'auto-biography' are 'secret' ones that for the most part escape the user's attention. This article explores how these sites of auto-biography reveal the complexities of the political economy of Web 2.0, as well as implicate an ethics of exposure concerning how these processes at once participate in the erosion of privacy, and at the same time, in the reinforcement of commodification and surveillance regimes.

Agenda:

Author:

Dr. Kenneth C. Werbin:

- Wilfrid Laurier University's Brantford Campus, 73 George St., Brantford, Ontario, N3T 2Y3. Canada.
- ☎ 519-756-8228 , ✉ kwerbin@wlu.ca
- Relevant publications:
  - Werbin, Kenneth C. Spookipedia: Intelligence, Social Media, and Biopolitics. Media, Culture & Society. SAGE Publications, Vol.33(8) 2011. 1254-1265
  - Werbin, Kenneth C. Fear and No-Fly Listing in Canada: The Biopolitics of the 'Aar on Terror'." The Canadian Journal of Communication, Vol.34(4) 2009. 613-634
  - Langlois, Ganaele, Fenwick McKelvey, Greg Elmer & Kenneth C. Werbin. Mapping Commercial Web 2.0 Worlds: Towards a Critical Ontogenesis. Fibreculture. Issue 14 2009.

ISSN 1614-1687

1 The Processes of Auto-Biography

Some years ago, while searching my own name on Google (sometimes referred to as 'ego-surfing'), I came across the website Zoominfo.com in my top search results. Upon visiting the site, I was surprised to discover that by mining and aggregating a series of strings of personal information and biographic data that I had left across the web, Zomminfo.com had not only automatically generated a curriculum vitae for me, but had also automatically situated me in a network of relations to others. The picture of me that Zoominfo.com continues to paint can be understood as a commodified form of auto-biography; one that involves not only self-representational practices—I generate content and represent myself on one site or platform—but also automated aggregation logics, wherein the self-representational content I produce is transformed into highly parsed and indexed bits of data that are open to endless recursive trajectories of circulation, recombination and commodification across indefinite sites and platforms.

In addition to Zoominfo.com, a variety of other automated self-representational platforms exist that not only aggregate biographic content from mainstream social media sites, like Facebook, Web 2.0, and the Web in general, but also tap into the vast storehouses of personal information contained in more difficult to access (but public) databases that general purpose search engine crawlers like those of Google do not reach (at least with respect to what is available to everyday end-users). The 'deep web' or 'invisible web' refers to the underlying subterfuge of the entire digital media ecology: the vast databases of the social, political, economic, and governmental infrastructure, including personal information contained in court and legal records, in the credit system, in securities and exchanges public records, in intelligence databases, as well as data from sites like Lexis Nexis, Amazon, Ebay and Date.com that are not generally captured by traditional search engines. In that regard, the commodified form of auto-biography that these sites produce emerges through a series of 'secret' processes that most likely escape the user's attention and awareness. Sites like Zoominfo.com, Pipl.com, 123people.com and Yasni.com not only continually mine and aggregate personal information from the (deep) web and beyond to represent the lives of people, but they also engage algorithmic networking logics to represent connections between them, increasingly capturing not only who people are, but whom they are connected to. Consider this from Pipl.com, which bills itself as the 'most comprehensive people search on the web':

> *"Unlike a typical search-engine, Pipl is designed to retrieve information from the deep web. Our robots are set to interact with searchable databases and extract facts, contact details and other relevant information from personal profiles, member directories, scientific publications, court records and numerous other deep-web sources. Pipl is not just about finding more results; we are using advanced language-analysis and ranking algorithms to bring you the most relevant bits of information about a person..."*[1]

In that regard, the term 'biographics' is deployed here to refer to the bits of personal information and biographic data that are mined and aggregated by these platforms; with the concept of 'auto-biography' speaking to how biographics circulate and are harvested as a commodified form in automated self-representational processes. As such, this article considers how sites of auto-biography, like Zoominfo.com, shed light on the complexities of the political economy of digital media in three ways: Firstly, highlighting the back and forth, invisible, or 'secret' nature of the processes of auto-biography; of how the act of representing oneself is inextricably intertwined with being represented in digital culture. Secondly, revealing the recursive nature of these processes, or how the commodity forms of 'biographics' and 'auto-biography' are ones that beget more commodities in the cascading processes of 'immanent commodification'[2]. And finally, implicating an ethics of exposure concerning how the processes of auto-biography at once participate in the erosion of privacy, and at the same time, in the reinforcement of intense commodification and surveillance regimes.

[1] http://pipl.com/help/deep-web/

[2] Mosco, Vincent: The Political Economy of Communication. 141

2 Back and Forth: The Immanent Commodification of Personal Information

There is a back and forth relationship that marks the processes of auto-biography outlined here: just as users produce and aggregate content to represent themselves, the content they generate and the data they produce are mined and aggregated to represent them. In other words, 'users are *created* by using'[3]. This is how Chun first described the back and forth transmission of 'involuntary representations'[4] that are endemic to participation in digital media. In line with the back and forth nature of such arrangements, Langlois et al. have argued that there is a 'double logic' inherent in how users are created by using in Web 2.0 worlds, with the 'processes of subjectivation'[5] by which user experience takes shape being marked by 'the inseparability of finding and being found, of locating ourselves and our personalized network'[6]. This is what Elmer also elaborated as the 'double articulation of locative media'[7], or 'the means by which users both locate information on networks and are themselves located'[8]. The processes of auto-biography outlined here are consistent with this double logic, where at the most minute level, the act of generating data can be seen as inseparable from being generated as data. Equally, the act of producing content is inseparable from being produced as content. Indeed, in the arrangements of auto-biography, to express is to be expressed, just as to self-represent is to be self-represented.

These double logics are part and parcel of the processes of commodification that underpin Web 2.0. The business model that is at the heart of these arrangements is fundamentally based on transforming the content and data generated by users into the commodity form[9]. In that regard, the back and forth, recursive logics associated with the processes of auto-biography align with what Mosco has described as 'immanent commodification', or 'how commodities produce their own new commodities'[10]. In the processes of auto-biography associated with the cascading nature of immanent commodification, the resources of personal information, self-representational content, and data related to patterns of interaction and communication are transformed into commodities that inherently possess the potential to be further commodified. This means that the biographics that users produce as they generate content and data possess potentials beyond the exchange value established between corporations like Google and Facebook and the advertisers and marketers with whom they do business, but also possess potentials to be commodified by external players, like Zoominfo.com, who scrape and mine the bowels of the (deep) web for these resources that are transformed into the aggregated commodity form of auto-biography.

In that regard, participation in Web 2.0 fundamentally involves a form of labor that is consistent with how Lazzarato has described 'immaterial labor', or 'labor that produces the informational and cultural content of the commodity'[11]. While there has been dispute over the exact term that should be applied to describe the kind of labor at play in Web 2.0 arrangements—with some applying the term 'immaterial labor'[12], others

[3] Chun, Wendy: Control and Freedom. 249

[4] ibid. 247

[5] Langlois, Ganaele, Fenwick McKelvey, Greg Elmer & Kenneth C. Werbin: Mapping Commercial Web 2.0 Worlds: Towards a Critical Ontogenesis.

[6] ibid.

[7] Elmer, Greg: Locative Networking: Finding and Being Found. 20

[8] ibid. 18

[9] See Vaidhyanathan, Siva: The Googlization of Everything.; van Dijck, Jose: Users like you? Theorizing agency in User-Generated Content; van Dijck, Jose & David Nieborg: Wikinomics and its Discontents: A Critical Analysis of Web 2.0 Business Manifestos

[10] Mosco, Vincent: The Political Economy of Communication. 141

[11] Lazzarato, Maurizio: Immaterial Labor. 133

[12] See Hardt, Michael & Antonio Negri: Multitude; Terranova, Tiziana: Network Culture: Politics for the Information Age; Coté, Mark & Jennifer Pybus: Learning to Immaterial Labour 2.0: MySpace and Social Networks;

opting for 'free labor'[13], and some for 'informational labor'[14]—there is nonetheless widespread agreement that corporate user-generated content arrangements involve exploiting users who produce the resources that are transformed into the commodity form. The commodified form of auto-biography that is momentarily stabilized on sites like Zoominfo.com is inextricably linked to these exploitative processes, leveraging the labor of users who produce the biographics that are ultimately assembled and commodified in these arrangements.

The double logic of the back and forth processes through which the form of auto-biography appears also aligns with what Mosco has described as the 'double mystification' of the commodity form: 'how it naturalizes the social relationship between capital and labor'[15], and at the same time is reified, taking on a life of its own 'that stands against the individual and society and comes to shape both'[16]. With regard to the former, it is the commodity form of auto-biography that appears on sites like Zoominfo.com (the curriculum vitae and network of relations) and not the struggle at the point of production over how much (or little, or nothing) user laborers are paid for their scraped information and data. With regard to the latter, the reified form of auto-biography carries credibility and authority to stand in for individuals, speaking to who they are, and whom they know a priori. In that way, the commodified form of auto-biography appears as 'a natural outcome of a production process, rather than the social consequence of a fundamental social struggle'[17] over the exploitative nature of Web 2.0 relations. In these exploitative arrangements, the reified form of auto-biography takes on a life of its own that is severed from the production processes through which it appears. 'The outcome of this double mystification is that the product of a social process is given an existence of its own and the power to mold social life'[18]. In that light, the commodified form of auto-biography appears not as the product of the processes of commodification, but as a credible, authoritative and fetishized representation of the individual with the power to mold and shape aspects of that individual's life.

A material analysis of these arrangements thus highlights how 'it is the production of audiences for the general capitalist economy that is central to the commodification process rather than the production of ideology'[19]. In that light, where those who have emphasized the participatory, active nature of users in these arrangements, arguing that the blurring of the lines between top-down forms of production and bottom-up practices of content generation have resulted in the empowerment of users[20], such approaches 'neglect to situate this process within a structure of decision-making that places in the hands of capital most, though not all, of the levers of control over decision-making about what gets produced, how it is distributed, and what it costs.'[21] While there is an understandable tendency to emphasize the creative potentials that social media open to individuals through the co-productive nature of Web 2.0, such emphasis also obscures the unevenness of the labor relations inherent in these arrangements. But for opting out of participation, users have very limited control over the production and circulation of biographics, how they are aggregated and

[13] See Andrejevic, Mark: Surveillance in the Digital Enclosure; Terranova, Tiziana: Network Culture: Politics for the Information Age; van Dijck, José: Users like you? Theorizing agency in User-Generated Content; van Dijck, José & David Nieborg: Wikinomics and Its Discontents: A Critical Analysis of Web 2.0 Business Manifestos

[14] See Fuchs, Christian: Internet and Society: Social Theory in the Information Age; Fuchs, Christian: Web 2.0, Prosumption, and Surveillance

[15] Mosco, Vincent: 132

[16] ibid.

[17] ibid.

[18] ibid.

[19] ibid.

[20] See Bruns, Axel: Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage; Burgess, Jean & Joshua Green: YouTube: Online Video and Participatory Culture; Deuze, Mark: Convergence Cultures in the Creative Industries; Gillmor, Dan: We the Media: Grassroots Journalism By the People, For the People; Howe, Jeff: Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business; Jenkins, Henry: The Cultural Logic of Media Convergence; Jenkins, Henry: Convergence Culture; Shirky, Clay: Here Comes Everybody: The Power of Organizing Without Organizations; Tapscott, Don & Anthony Williams: Wikinomics: How mass collaboration changes everything;

[21] Mosco, Vincent: 138

commodified in the processes of auto-biography, and what aspects of their lives are monitored and tracked. As such, users are not only the products of these arrangements, but are also the subjects of surveillance that is a necessary condition of the back and forth, recursive logics that mark the appearance of the commodified form of auto-biography. In that regard, commodification and surveillance operate hand-in-hand in the processes of auto-biography: a double articulation of the logic of both.

3 An Ethics of Exposure: Where Privacy Meets Auto-Biography

> *"Immanent commodification not only produces new commodities; it creates powerful surveillance tools that threaten privacy"*[22]

Clearly, the erosion of privacy inherent in digital culture is of critical concern as evidenced by an increase in scholarship related to how current arrangements, including conjunctions of wireless devices, CCTV, facial recognition technology, biometrics, GPS, cookies, and search engine technologies, pose severe threats to privacy[23]. Moreover, this increase in scholarship runs in parallel to more and more stories appearing in mainstream media reporting on the unforeseen use of personal information harvested from across the social web[24].

In their examination of Canadian privacy policy and discourse, Shade and Shepherd[25] have articulated 'immanent commodification' with the concept of 'contextual integrity' that Nissenbaum advances in her analysis of informational privacy[26]. Contextual integrity is 'defined as compatibility with presiding norms of information appropriateness and distribution'[27]. In Shade and Shepherd's analysis, the variable nature of digital arrangements means that questions of control over personal information and violations of privacy are 'situationally dependent' involving 'the role of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination'[28]. The momentarily stabilized and commodified form of auto-biography is the situationally dependent product of just such relations and terms and conditions that for the most part remain invisible to users despite the exploitation of their labor and infringements of their privacy. Contextual integrity applied as such challenges, 'whether socio-technical devices, systems, and practices affecting the flow of personal information in a society are morally and politically legitimate'[29]. In that light, the contextual integrity of the commodified form of auto-biography is a dubious one at best, playing out on a digital terrain that is rife with ethical complications that pivot around privacy, the circulation of personal information, and exposure.

In the broadest sense, the commodified forms of biographics and auto-biography participate in the unsettling of 'freedom of expression'. Wacks has argued that in digital culture the awareness that one might be watched anytime and anywhere challenges people's subjective and emotional autonomy, altering what they are (or are not) willing to do or say[30]. In Web 2.0 arrangements, the freedom to express oneself is inextrica-

---

[22] Mosco, Vincent: 143

[23] See Bennett, Colin J.: The Privacy Advocates; Mosco, Vincent; Nissenbaum, Helen: Privacy in Context; Vaidhyanatahn, Siva; Wacks, Raymond: Privacy: A Very Short Introduction; Zimmer, Michael: 'The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0'

[24] See Dabu, Nonato: Employers requesting Facebook password violates privacy; Dyson, Esther: How Loss of Privacy May Mean Loss of Security; El Akkad, Omar & Susan Krashinsky: The See-Through Society; Jeffries, Stewart: G2: Life Through a Lens; Stolove, Daniel: Do Social Networks Bring the End of Privacy?; Rosen, Jeffrey: The Web Means the End of Forgetting;

[25] Shade, Leslie R. & Tamara Shepherd: Tracing and Tracking Canadian Privacy Discourses: The Audience as Commodity

[26] Nissenbaum, Helen: Privacy as Contextual Integrity

[27] ibid.: 137

[28] ibid.: 137-138

[29] Nissenbaum, Helen: Privacy in Context: 236

[30] Wacks, Raymond

bly intertwined with the production of information that always possesses the potential to be personally identifiable when taken up in commodification and surveillance regimes. Even in instances where information and data produced are considered anonymous, when correlated with other such data, what is thought to be non-identifiable can quickly become personally identifiable. This means that the data people produce, even anonymously, might be leveraged and aggregated at any time to represent their lives in unexpected and identifiable ways. Whether people limit what they are willing to do or say with this knowledge, or play up to surveillance by exaggerating their words and behaviors to gain recognition, the awareness that one's expression and data might be aggregated at anytime has profound implications with regards to what people are (or are not) willing to do or say.

The reification of the commodified form of auto-biography, standing in for people a priori and possessing the power to open and close opportunities available to them also presents profound ethical complications. The processes of auto-biography are fundamentally built on the logic of 'social sorting', classifying people according to criteria and sorting them into categories[31]. As Lyon argues, categories and classes of people are inherently political and call for ethical inspection[32]. As Gandy tells it, the ways that people are included and excluded through data-mining and sorting logics 'rationalizes discrimination in the broadest sense…in the 'rational pursuit of profits'[33]. Moreover, the production of inaccuracies through routine 'dataveillance'[34] heightens these ethical quandaries. Both Haggerty & Ericson, and Bennett have concluded that data surveillance inherently produces inaccuracies and errors that can have very real consequences for people's lives, namely their exclusion from opportunities.

Overall, in current digital arrangements, privacy is increasingly transformed from a right into a commodity, where maintaining one's anonymity and managing one's reputation comes at a cost. The processes of auto-biography as such do not merely align with Mosco's notion of 'immanent commodification', but also factor in 'external commodification', or '…a process of expansion that extends commodification to areas that, for a range of social, political, cultural, and economic reasons, were historically left outside the process or only lightly affected by it'[35]. Indeed, anonymizing software and reputation management services are privacy commodities that emerge in arrangements where users are created by using, produced by producing, expressed by expressing, and self-represented by self-representing. As such, the processes of auto-biography further reinforce the conjunction and expansion of digital capitalism, commodification and surveillance; a subject that demands vigilant ethical attention.

In short, the ethical complications of the arrangements of auto-biography implicate an ethics of exposure. How deep is too deep with respect to the kinds of personal information that can be aggregated, commodified and exposed by sites and platforms? While the information that is harvested from the deep web is technically in the public domain (e.g. information contained in court and legal records), an ethics of exposure challenges the moral and political legitimacy of the unbridled free flow of personal information contained in the vast databases of our social, political, economic, and governmental infrastructure. This involves asking questions like whether or not the details of a divorce case or lawsuit should circulate with the same ease as the more mundane details of a person's personal and professional life. An ethics of exposure, as such, revolves around considerations of privacy and the circulation, aggregation, and exposure of personal information; interrogating the terms by which sites gather and expose personal information, their relationship to and with the subjects they represent, the terms by which personal information will be further accumulated, disseminated and commodified, and how they have acquired, or at the very least, sought to acquire informed consent from their subjects about the self-representations that are being made on their behalf.

[31] Lyon, David: Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination

[32] ibid.

[33] Gandy, Oscar: Data Mining and Surveillance in the post 9/11 environment: 153

[34] Haggerty, Kevin D. & Richard V. Ericson: The New Politics of Surveillance and Visibility

[35] Mosco, Vincent: 143

In conclusion, sites of auto-biography, like Zoominfo.com, highlight the complexities of the political economy of Web 2.0 in three ways: Firstly, these sites exemplify the back and forth logic of these arrangements, wherein the act of representing oneself is inextricably intertwined with being represented. Secondly, these sites reveal the recursive nature of these arrangements, or how the commodity forms of 'biographics' and 'auto-biography' are ones that are part and parcel of the cascading processes of 'immanent commodification'. Finally, these sites illuminate the ethical complications of the processes of auto-biography, that at once participate in the erosion of privacy, and at the same time, in the reinforcement of commodification and surveillance regimes. Indeed, the processes and sites of auto-biography outlined here implicate an ethics of exposure that must be grappled with if we are to come to terms with how our lives (and how they are told) are increasingly both the products of commodification and the subjects of surveillance.

Acknowledgments

This research was funded by the Social Sciences and Humanities Research Council of Canada, Wilfrid Laurier University and Ryerson University. The author would like to thank Greg Elmer, Ganaele Langlois, Fenwick McKelvey and Leslie Regan Shade for their thoughts and conversations.

References

Andrejevic, Mark: Surveillance in the Digital Enclosure. In S. Magnet and K. Gates (eds). The New Media of Surveillance. London and New York, Routledge 2009. 18-40

Bennett, Colin J. The Privacy Advocates. Cambridge, MA, MIT Press 2008.

Bruns, A. Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage. New York, Peter Lang 2008.

Burgess, Jean and Joshua Green. YouTube: Online Video and Participatory Culture. Cambridge, UK, Polity Press 2009.

Chun, Wendy H.K. Control and Freedom: Power and Paranoia in the Age of Fiber Optics. Cambridge, Mass, MIT Press 2006.

Coté, Mark and Jennifer Pybus. Learning to immaterial labour 2.0: MySpace and social networks. Ephemera 7(1), 2007. 88-106

Dabu Nonato, Sheila. Employers requesting Facebook password violates privacy. Postmedia News. Canada, 2012, March 21. Retrieved from:

http://www.canada.com/Employers+requesting+Facebook+password+violates+privacy+Experts/6339360/story.html

Deuze, Mark. Convergence Cultures in the Creative Industries. International Journal of Cultural Studies Vol.10(2). SAGE Publications 2007. 243-263.

Dyson, Esther. How Loss of Privacy May Mean Loss of Security. In Scientific American Special Issue on "The Future of Privacy". August 2008. Retrieved from: http://www.sciam.com/article.cfm?id=how-loss-of-privacy-may-mean-loss-of-security

El Akkad, Omar & Susan Krashinsky. The See Through Society. The Globe and Mail. Toronto, CTVglobemedia Publishing 2010.

Elmer, Greg. Locative Networking: Finding and Being Found. Aether: The Journal of Media Geography. Vol. v.a., 2010. 18-26

Fuchs, Christian. Internet and society: Social theory in the information age. New York, Routledge 2008.

Fuchs, Christian. Web 2.0, Prosumption, and Surveillance. Surveillance & Society 8(3), 2011. 288-309

Gandy, Oscar H. Data Mining and Surveillance in the post 9/11 environment. In S.P. Hier & J. Greenberg (Eds.), The surveillance studies reader. New York, Open University Press 2007. 147-157

Gillmor, Dan. We the media: grassroots journalism by the people, for the people. Sebastopol, CA, O'Reilly 2004.

Haggerty, Kevin D. & Richard V. Ericson. The New Politics of Surveillance and Visibility. Toronto, University of Toronto Press 2006.

Haggerty, Kevin D. & Minas Samatas. Surveillance and Democracy. New York, Routledge 2010.

Hardt, Michael and Antonio Negri. Multitude. New York, Penguin Press 2004.

Hofmann, Marcia. EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites. Electronic Frontier Foundation, Deep Links Blog March 16, 2010. Retrieved from:
http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement

Howe, Jeff. Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business. New York, Crown Business 2008.

Jeffries, Stewart. "G2: Life Through a Lens. The Guardian. London, UK, January 8, 2010. 4

Jenkins, Henry. The Cultural Logic of Media Convergence. International Journal of Cultural Studies. 7(1). 2004. 33–43.

Jenkins, Henry. Convergence Culture. New York, New York University Press 2006.

Langlois, Ganaele, Fenwick McKelvey, Greg Elmer & Kenneth C. Werbin. Mapping Commercial Web 2.0 Worlds: Towards a Critical Ontogenesis. Fibreculture. Issue 14 2009.

Lazzarato, Maurizio. Immaterial Labor. In Virno, P. & Hardt, M. (eds.) Radical thought in Italy. Minneapolis, MN, University of Minnesota Press 1996. 133-146

Lyon, David. Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.New York, Routledge 2003.

Mosco, Vincent. The political economy of communication (2nd ed.). Los Angeles, SAGE 2009.

Nissenbaum, Helen. Privacy as Contextual Integrity. Washington Law Review 79(1) 2004. 101-139

Nissenbaum Helen. Privacy in Context. Stanford, CA, Stanford University Press 2010.

Rosen, Jeffrey. The Web Means the End of Forgetting. The New York Times. New York, NY, July 21 2010.

Schachtman, Noah. U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets. Wired Magazine. October 2009.

Shade, Leslie Regan and Tamara Shepherd. Tracing and Tracking Canadian Privacy Discourses: The Audience as Commodity. In Kozolonka, Kirsten (ed.) Publicity and the Canadian State. Toronto, University of Toronto Press Forthcoming 2013.

Shirky, Clay. Here Comes Everybody: The Power of Organizing Without Organizations. New York, Penguin Books 2008.

Tapscott, Don & Anthony D. Williams. Wikinomics: How Mass Collaboration Changes Everything. London, Penguin Press 2006.

Stolove, Daniel J. Do Social Networks Bring the End of Privacy. In Scientific American Special Issue on "The Future of Privacy". August 2008.

Terranova, Titziana. Network Culture: Politics for the Information Age. London, Pluto Press 2004.

Vaidhyanathan, Siva. The Googlization of Everything (and why we should worry). Berkeley, CA, University of California Press 2011.

van Dijck, José. Users Like You? Theorizing Agency in User-Generated Content. Media, Culture & Society, 31(1) 2009. 41-58.

van Dijck, José & David Nieborg. Wikinomics and Its Discontents: A Critical Analysis of Web 2.0 Business Manifestos. New Media & Society, 11(5) 2009. 855-874.

Wacks Raymond. Privacy: A Very Short Introduction. Oxford, Oxford University Press 2010.

Zimmer, Michael. The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0. First Monday, 13(3) 2008.