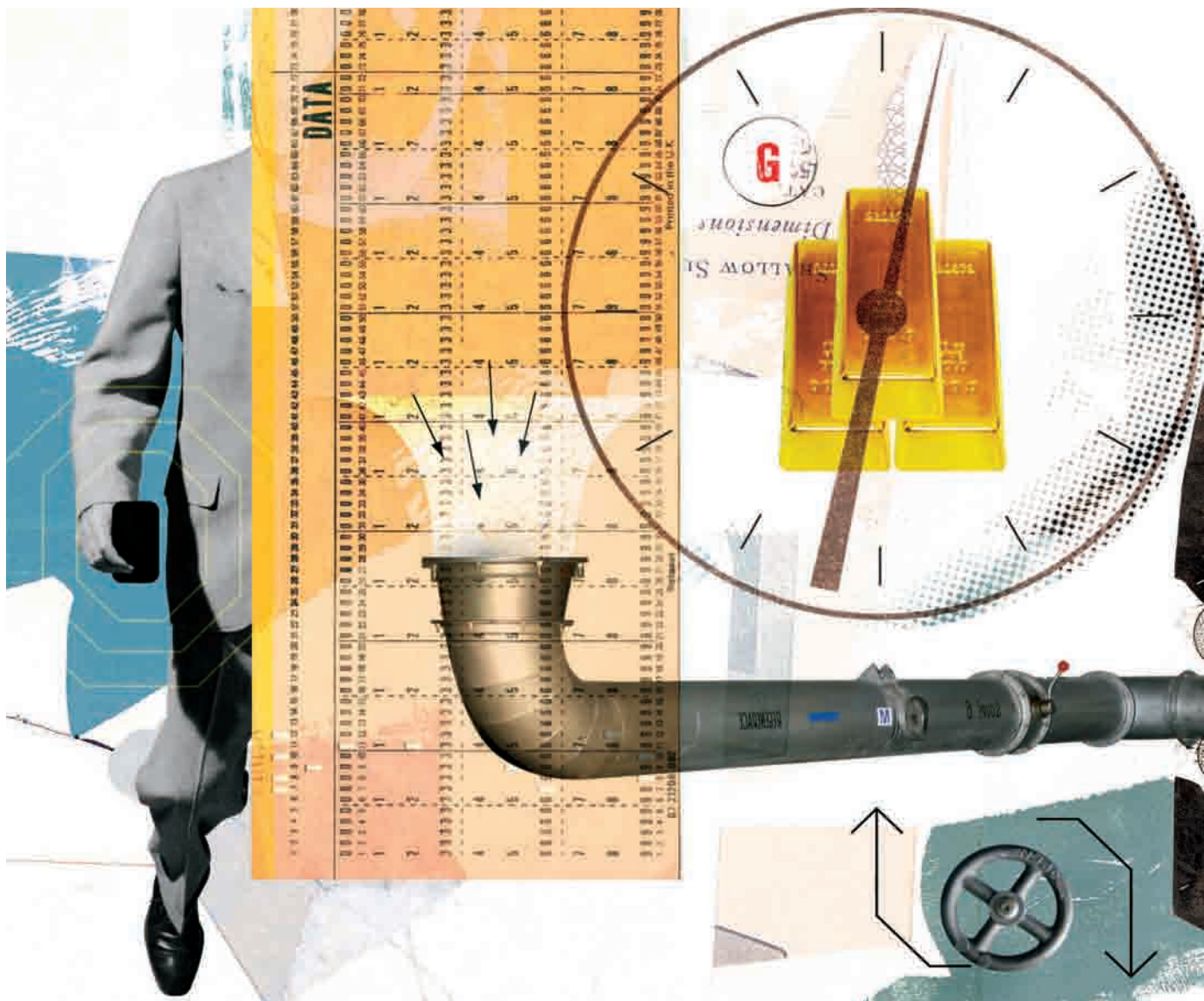


## Il valore della Privacy

Prima ancora che un problema di carattere etico, la privacy rappresenta un campo di interessi che cresce ogni giorno a ritmi vertiginosi e appare sempre più complesso. Le informazioni private stanno diventando dei fattori cruciali negli orientamenti del mercato, negli investimenti pubblicitari, negli stessi processi decisionali di carattere sociale e politico. Tutto ciò richiede nuovi modelli commerciali e nuove tecnologie in grado di modulare il sistema secondo i mutevoli interessi e le sensibilità del mercato. Altrettanto ineludibile è il confronto tra tutte le parti in gioco, perché le aziende interessate sanno bene quanto possa rapidamente capovolgersi l'atteggiamento dei loro utenti, soprattutto quando si sentono, per così dire, colpiti sul vivo.



## Privacy su Internet?

Servizi gratuiti in cambio di informazioni personali: questo è il contratto che tutti sottoscriviamo su Internet. Ma potrebbe rivelarsi un pessimo affare.

**Cory Doctorow**

**E**cco una storia su Internet di cui avete sentito parlare: barattiamo la nostra privacy in cambio di servizi. Il concetto è che i nostri dati personali hanno per noi meno valore di quanto lo abbiano per le aziende che li sottraggono dal nostro browser, mentre navighiamo in rete. Loro sanno cosa farne per trasformarli in qualcosa di prezioso, per sé e per noi. Questa vicenda ha assunto dimensioni mitiche e ciò non deve meravigliare, dal momento che sono coinvolti miliardi di dollari.

Ma se di accordo si tratta, allora si tratta di un curioso accordo unilaterale. Per comprendere che tipo di contratto sottoscrivete sulla vostra privacy un centinaio di volte al giorno, vi invito a leggere e a condividere quanto segue: «Con la lettura di questo accordo riconoscete da ora in avanti a TR e ai suoi soci il diritto illimitato di intercettare ed esaminare le vostre scelte di lettura, di vendere di conseguenza i dati raccolti, di conservare questo tipo di informazioni per sempre e di cederle a terzi senza alcun limite».

In verità il testo sopra riportato non è esattamente identico ai termini con i quali sottoscriviamo un accordo ogni volta che clicchiamo sul mouse. Per rendere effettivamente compiuta la similitudine, dovrei chiedere a questa rivista di nascondere questo testo a margine di una delle ultime pagine e dovrei terminarlo con la seguente frase: «Questo accordo è soggetto a modifiche in qualunque momento». Ciò che decidiamo di sottoscrivere su Internet non è negoziabile. È come una sorta di rinfresco, dove i fatti privati della nostra vita sono il buffet.

Perché sembriamo dare così scarso valore alla privacy? In parte perché ci

viene detto di farlo. Facebook, più di una volta, ha disatteso le preferenze dei propri utenti in materia di privacy, sostituendole con nuove configurazioni predefinite. Poi ha risposto all'inevitabile protesta di massa reintegrando qualcosa di simile al vecchio sistema, solo leggermente meno privato e aggiungendo poche righe in più a un indecifrabile e complesso sistema di controllo sulla privacy. Pure leggendo le clausole scritte in piccolo, le persone hanno una scarsa capacità di valutare nel presente la reale portata di una decisione, le cui conseguenze sono proiettate nel futuro. Nessuno inizierebbe a fumare se i tumori insorgessero alla prima boccata di fumo. Allo stesso modo la grande parte delle note informative sulla privacy non ci provocano uno stress fisico ed emotivo immediato. Ma è un dato di fatto che, se molte persone rivelano una grande quantità di informazioni riservate, il danno è certo. Tutti abbiamo sentito parlare di storie di persone licenziate per aver messo il flag sbagliato sulla mail in cui si lamentavano del lavoro.

Il rischio aumenta quante più informazioni riveliamo, proprio come siamo indotti a fare dall'impostazione dei social network. Quando si comincia la propria vita in un nuovo social network, veniamo ricompensati con un rinforzo sociale, poiché spuntano fuori vecchi amici che si congratulano con noi per esserci uniti alla festa. Ulteriori rivelazioni di carattere personale generano altre ricompense, ma non sempre. Alcune rivelazioni possono sembrarvi delle notizie bomba («Sto divorziando»), ma fuori dal vostro social network producono soltanto un frinire virtuale di grilli. Tuttavia notizie apparentemente insignificanti («Con questi jeans il mio sedere sembra grosso?») possono causare un fiume di risposte. Gli scienziati del comportamento hanno dato un nome a questa dinamica: «rinforzo intermittente». Si tratta di una delle più efficaci tecniche di training comportamentale che conosciamo. Date a un topo di laboratorio una leva che produce una pallina di cibo ogni volta che viene azionata e vedrete che l'azionerà solo quando è affamato. Dategli una leva che produce palline di cibo a intervalli casuali e lui la terrà sempre azionata.

Quali sono i progressi della società in tema di tutela della privacy? Come ha

indicato Lawrence Lessig nel suo libro *Code and Other Laws of Cyberspace*, esistono quattro potenziali strumenti: le norme, la legge, il codice e i mercati. Sino a oggi siamo stati abbastanza scarsi su tutti i fronti. Prendiamo la norma: il nostro principale strumento di regolamentazione per migliorare le decisioni in tema di privacy è una sorta di monito indulgente rivolto principalmente ai bambini: «Passi troppo tempo su questi siti!» Eppure le scuole, le biblioteche e i genitori sfruttano gli *spyware* della rete per catturare tutti i click, gli aggiornamenti di profilo e le chat dei ragazzi allo scopo di proteggerli dagli altri adulti. In altre parole: la vostra privacy è infinitamente preziosa fintanto che non la violate (E se fate qualsiasi cosa per eludere la nostra protezione di rete, siete in guai seri). E per quanto riguarda la legge? Negli Stati Uniti vige un uso consentito per qualcosa che viene chiamato «Do Not Track»: gli utenti possono impostare i loro programmi di navigazione in modo che venga inviato un avviso del genere: «Vietato raccogliere informazioni sul mio utente». Ma non sono previsti sistemi di riscontro all'interno, non si ha la certezza del corretto funzionamento a meno che gli utenti non piombino negli sconfinati centri informatici per assicurarsi che non stiano imbrogliando. Agli europei piace pensare di possedere i propri dati, ovvero di avere un diritto di proprietà sulle vicende riguardanti la propria vita e il diritto di pretendere che questa «proprietà» non venga violata. Ma anche questo approccio è inadeguato. Se c'è una cosa che gli ultimi 15 anni di battaglie sulla normativa per Internet ci hanno insegnato, è che non si giunge mai a una soluzione attribuendo alle informazioni copiate facilmente i diritti analoghi a quelli della proprietà.

Per quanto riguarda il codice c'è ancora margine di miglioramento e di profitto. Una buona parte dei dati raccolti in Internet è il risultato delle impostazioni permissive riguardo alla modalità con la quale i nostri browser trattano i cookie, ovvero frammenti di codice usati per identificarci. A oggi ci sono due modalità di navigazione in rete: disattivare del tutto le funzioni dei cookie e convivere con il fatto che molti siti non si apriranno o permettere l'accesso a tutti i cookie, accettando così il totale



trafugamento delle vostre abitudini di navigazione.

I produttori di browser potrebbero puntare il dito sulla questione. Come precedente, pensiamo a cosa è successo alla pubblicità pop up. Quando la rete era ancora giovane, i pop up erano ovunque. Comparivano in piccole finestre che risbucavano fuori ogni volta che venivano chiuse, sfuggendo al cursore ed emettendo musica. Poiché i pop up erano l'unico mezzo per ottenere un prezzo ragionevole dai pubblicitari, era opinione diffusa che i produttori di browser non avrebbe potuto permettersi di bloccare i pop up per default, malgrado gli utenti li detestassero.

L'impasse fu superata da Mozilla, una organizzazione no profit che si preoccupava principalmente di dare un

servizio agli utenti e non ai proprietari di siti o ai pubblicitari. Quando Firefox di Mozilla attivò il dispositivo di blocco dei pop up, cominciò a riscuotere un enorme successo. Gli altri produttori di browser non ebbero altra scelta se non quella di seguirne l'esempio.

I prossimi saranno gli amministratori di cookie. Immaginate se il vostro browser consentisse l'accesso solo ai cookie che ritiene utili a voi, piuttosto che alle dozzine di cookie provenienti da siti pubblicitari con i quali non avete mai avuto l'intenzione di interagire. I pubblicitari e i buyer sostengono che l'idea non può funzionare. Ma la verità è che l'abolizione della tracciabilità su Internet non segnerà la fine della pubblicità. Alla fine potrebbe costituire un cambiamento positivo sia per gli analisti, sia per i pubblicitari.

Oggi si ha la sensazione che chiunque possa sottrarre informazioni dal vostro computer, incurante di fornire un buon servizio. Una volta che l'accordo sulla privacy venisse stipulato senza alcuna coercizione, le aziende corrette potrebbero realizzare servizi in grado di ottenere molte più informazioni dai propri utenti, rispetto a quelle senza scrupoli.

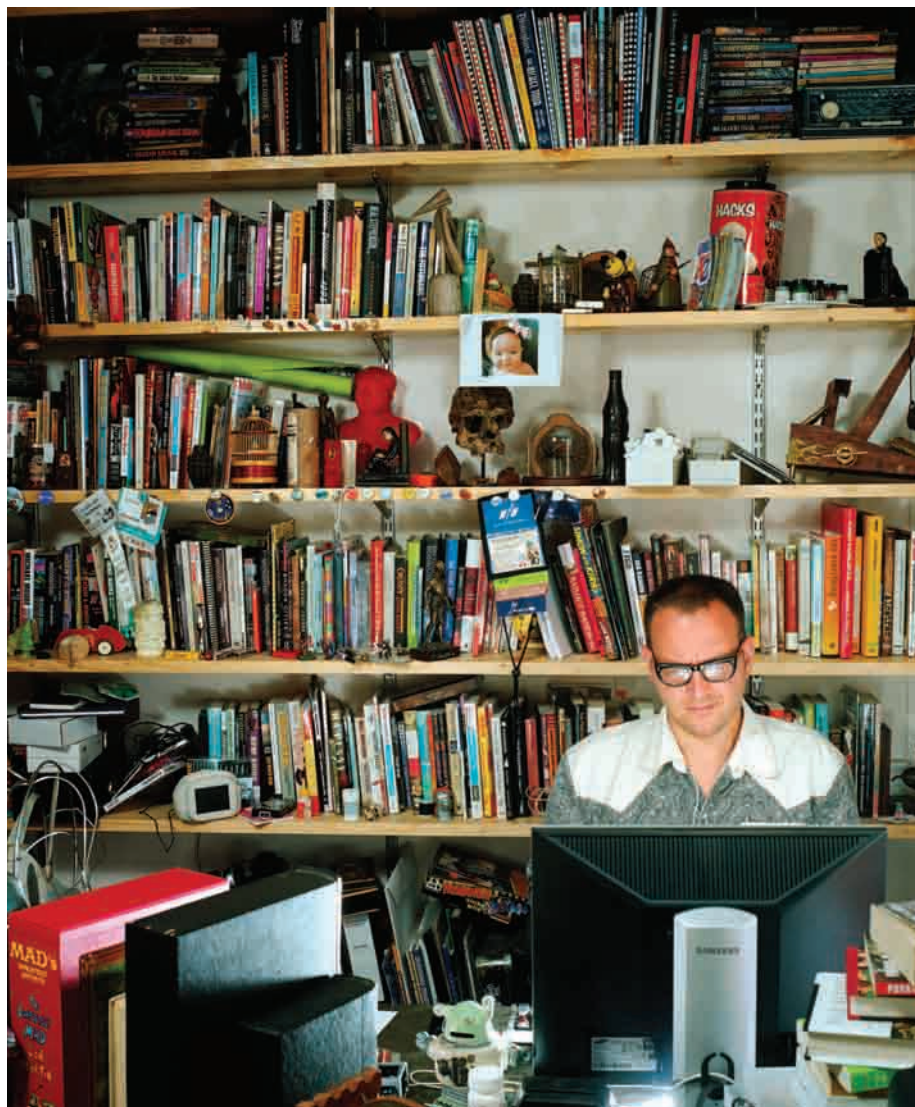
Per quanto riguarda i dispositivi mobili, occorrerebbe una strumentazione più sofisticata. Oggi il mercato degli applicativi destinati agli apparecchi mobili propongono offerte del tipo "prendere o lasciare". Se volete scaricare l'applicativo Connect the Dots per intrattenere i vostri bambini durante un lungo viaggio in auto, è necessario fornire all'applicativo l'accesso al vostro numero di telefono e alla vostra posizione. Cosa accadrebbe se i terminali Os fossero progettati per consentire ai loro utenti di mentire agli applicativi? «Tutte le volte che l'applicativo Connect the Dots vuole sapere dove vi trovate, inventatevi qualcosa. Quando vi chiede il vostro numero di telefono, datene uno a caso». Un modulo sperimentale di Cyanogenmod (una versione gratuita/aperta dell'Android Os) già lo fa. Funziona abbastanza bene, ma potrebbe andare meglio se fosse sostenuto ufficialmente da Google.

Lungi dal penalizzare il settore, il controllo da parte degli utenti delle informazioni riservate creerebbe valore aggiunto. Progettate dunque un applicativo a cui possa fornire volontariamente la mia posizione e sarete una delle poche aziende ad avere il mio consenso per entrare in possesso di questa informazione e rivenderla. Oggi gli utenti e gli analisti sono in guerra, ma solo gli analisti sono armati. Questa è una buona opportunità di business per un'azienda che voglia fornire armi ai ribelli piuttosto che all'impero. **TR**

*Cory Doctorow, giornalista e codirettore di "Boing Boing", si occupa di letteratura scientifica.*

**Cory Doctorow al lavoro nella privacy del suo studio di Londra.**

*Fotografia: Jonathan Worth / Creative Commons*



## Chi ha torto e chi ha ragione?

Microsoft e i suoi concorrenti presentano importanti differenze quando si tratta di proteggere le informazioni personali. Così afferma Brendon Lynch, responsabile della normativa sulla privacy di Microsoft.

**Lee Gomes**

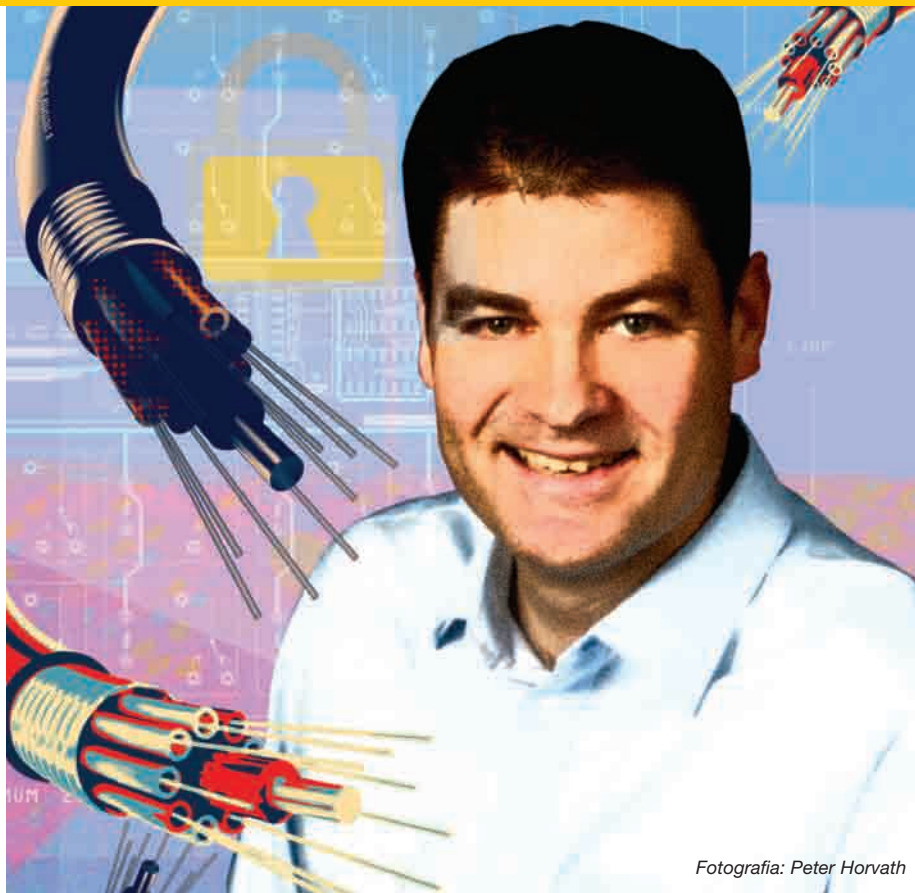
All'inizio di quest'anno, Microsoft ha fatto scalpore pubblicando in un importante quotidiano alcune dichiarazioni che accusavano il suo principale rivale, Google, di calpestare la privacy individuale attraverso la raccolta sempre più massiccia di informazioni sugli utenti. Alcuni hanno ritenuto ipocrite queste dichiarazioni: Microsoft si avvale di strumenti analoghi con il proprio motore di ricerca, Bing. Ma in Microsoft, la rivendicazione della propria supremazia in fatto di tutela della privacy è un dogma. A partire dagli anni Novanta, Microsoft ha avviato la propria battaglia contro le lacune in tema di sicurezza all'interno del proprio sistema operativo Windows. Prima, privacy significava proteggere il proprio computer dal virus di qualche pirata informatico. Oggi è sinonimo di un uso corretto dei nostri dati personali da parte delle aziende.

### Perché Microsoft ha criticato Google?

Si stava rendendo conto che c'era inquietudine nell'ambiente, che c'era preoccupazione fra molti utenti in fatto di privacy. Siamo molto fieri del modo in cui realizziamo sistemi e controlli sulla privacy e volevamo che le persone sapessero che c'è un'alternativa.

### Bing di recente ha consentito agli utenti di registrarsi con Facebook e di condividere i risultati di ricerca. Ai social media riservate un trattamento in qualche modo diverso?

Le persone devono scegliere di partecipare a qualsiasi esperienza in cui i risultati della ricerca vengano condivisi. Inoltre Facebook



Fotografia: Peter Horvath

richiede che per accedere ai propri servizi gli utenti abbiano almeno 13 anni, mentre i motori di ricerca sociale di Bing permettono la consultazione dei dati solo agli utenti di almeno 18 anni.

### Che cosa ha imparato Microsoft durante gli anni Novanta, quando i teorici della cospirazione vi hanno accusato di usare gli aggiornamenti di Windows per spiare le persone?

Questa accusa ci ha realmente aiutato a capire l'importanza della fiducia. Gli aggiornamenti di Windows consentono di proteggere la società dalle minacce on line. Così abbiamo voluto sottolineare i solidi controlli sulla privacy presenti in Windows Update, in modo che le persone avessero fiducia e lo usassero. Una delle cose che abbiamo fatto è stata quella di invitare uditori indipendenti, che potevano muoversi in mezzo a tutto quanto facevamo e che alla fine stendevano dei rapporti per rassicurare chiunque che stavamo raccogliendo solo i dati concordati.

### Oggi la privacy significa qualcosa di diverso per Microsoft rispetto a quanto significava 15 anni fa?

La sicurezza, poiché ha che fare con le informazioni, riguarda essenzialmente la

protezione di queste informazioni, ma la privacy è un concetto molto più ampio: qual è l'uso corretto delle informazioni?. Già all'inizio in Microsoft c'era molta attenzione per la privacy, ma nel corso degli ultimi dieci anni abbiamo accresciuto gli investimenti per arrivare pronti al momento in cui la privacy sarebbe diventata un tema importante. La grande sfida del nostro tempo in tema di privacy sarà quella di permettere alla società di trarre vantaggio dalle innovazioni basate sulla raccolta di informazioni e di assicurare al contempo che la privacy individuale venga protetta.

### Dispositivi come il controller del gioco Kinect presentano nuove sfide in tema di privacy?

Ci sono effettivamente alcuni aspetti sensibili al tema della privacy: per esempio il riconoscimento vocale e quello del volto. La tutela della privacy, in questo caso, richiedeva la certezza che nessuna di queste informazioni avrebbe abbandonato il dispositivo Kinect. Ma questo non significa non raccogliere informazioni o condividerle con gli altri. **PR**

*Lee Gomes, già collaboratore di "Forbes Magazine", è uno scrittore freelance.*