Governmental surveillance threatens client privacy

Samuel D. Lustgarten

The University of Iowa

Author Note

Samuel D. Lustgarten, Counseling Psychology, Department of Psychological and Quantitative Foundations, The University of Iowa.

Corresponding Author: Samuel D. Lustgarten, Counseling Psychology, Department of Psychological and Quantitative Foundations, The University of Iowa, 361 Lindquist Center, Iowa City, Iowa, 52242-1529, USA. E-mail: Samuel-Lustgarten@uiowa.edu
Acknowledgements: Dr. Elizabeth Altmaier, Dr. Stewart Ehly, Daniel Elchert, and Micah Lee.
Governmental surveillance threatens client privacy

Over the last two decades, the field of psychology has appreciated from technological progress. Practitioners are using text messaging (Norcross, Pfund, & Prochaska, 2013) and email (Shapiro & Schulman, 1996) for extended client care. Colbow (2013) found that psychologists and helpers are showing growing interest in telemental health therapy (remote therapy), which necessitate teleconferencing programs (i.e., Skype or Google Hangouts).

Each program and technology has consequences for client privacy and confidentiality. To manage risk associated with maintaining digital records and communication with clients, the American Psychological Association (APA) issued two documents: the “Ethical Principles of Psychologists and Code of Conduct” (2010; hereafter referred to as, “Ethics Code”) and “Record Keeping Guidelines” (2007). These documents place responsibility for confidential record management with psychologists.

Unfortunately, the ability for psychologists to maintain privacy and confidentiality in the twenty-first century is threatened. The evolution of technology combined with governmental surveillance and policy has led to vulnerabilities in digital maintenance of client records. This article reviews the current governmental threats to privacy and provides 5 best practices for securing information.

The NSA, Cloud Storage, and Electronic Communications

Various national agencies conduct surveillance in the service of state interests. Relevant to the current article is the National Security Agency (NSA; 2011), which is primarily tasked...
with collecting signals intelligence (from foreign sources). Until recently, it was believed that domestic surveillance was considered unlawful.

In June 2013, Glenn Greenwald took possession of top-secret documents from governmental whistleblower, Edward Snowden (Greenwald, 2014). The articles, known as “The NSA Files,” catalogued covert surveillance operations that extended into the U.S. (Greenwald, 2013). With the help of Snowden and other journalists, Greenwald (2013) first published evidence that the NSA was demanding and receiving “records of millions of Verizon customers daily.”

One program – “MUSCULAR” – allowed NSA analysts to access cloud storage networks of companies such as Google and Yahoo (Gellman & Soltani, 2013). This enabled the NSA to download and retrieve private information of U.S. citizens using cloud-based services (i.e., Gmail, Google Drive, and Yahoo Mail). It is possible the NSA could have retrieved private health information (PHI), notes, and work logs. If a provider and client emailed back and forth, the NSA could have accessed this information. These policies hinder psychologists’ ability to uphold the APA Ethics Code (2010), which states, “Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stores in any medium.”

Top-secret programs are only one type of governmental threat to privacy. The Stored Communications Act of 1986 (18 U.S. Code § 2703) allows the federal government to access cloud-based email when left on servers over 180 days. When the Act was signed, the popular method for email was to download messages to local computers –removing it from servers. Now, people tend to archive messages, rather than downloading or deleting (Google, 2014). With
corporations providing high-capacity cloud services, communications with clients that are saved, archived, and/or left on servers are vulnerable to government data requests.

Governmental surveillance and access to communications is easier at public institutions. Anyone can make Freedom of Information Act requests (FOIA; 5 U.S. Code § 552), and ask for the emails of faculty and staff. For instance, while communications between practitioners and clients is considered privileged information, emails between other practitioners and in indirect support of clients may not be protected (University of Iowa, 2013).

Lastly, mental health providers have a duty to explain to clients about requests for confidential information (ethics code citation). The Federal Bureau of Investigation (FBI) may have the authority to issue National Security Letters (NSLs) to request client records (18 U.S. Code § 2709). NSLs may necessitate that the recipient not notify persons involved, thus limiting the ability for practitioners to share about investigations affecting clients.

Best Practices for Client Confidentiality

The APA Ethics Code (2010) suggests that failure to maintain confidentiality and related ethical standards may result in legal consequences (Benefield, Ashkanazi, & Rozensky, 2006; Glosoff, Herlihy, Herlihy, & Spence, 1997). While the APA (2007; 2010) provides standards and guidelines for the use of data, best practices are absent. Despite the aforementioned threats to client privacy and confidentiality, there are methods to manage risk of unintended disclosures. The following section outlines 5 best practices for maintaining client confidentiality.

1. Create a threat model

Practitioners should anticipate security threats. While challenging to predict every concern, practitioners can develop “threat models” (Barrows & Clayton, 1996; Lee, 2013).
Threat models consider client populations (i.e., low, moderate, and high risk). By grouping clients into different risk categories, practitioners can create greater protections when necessary (i.e., LGBT-identified clients, dissidents, politicians, and celebrities). Practitioners’ threat models should be inversely related to risk: high-risk populations met with lower-tech mediums.

2. Encrypt everything

Practitioners should research encryption software to protect welfare. The APA Practice Organization (2014) catalogued three different types of options for client records: full-disk, virtual-disk, and file encryption. Full-disk encryption provides protection for the entire file system, and prevents organizations from files. If providers are interested in backing up and storing client records on HIPAA-compliant cloud-storage servers, files should be encrypted prior to uploading via virtual-disk encryption. Micah Lee (personal communication, September 28, 2014), technologist for The Intercept, provided four suggestions: disk encryption, firewalls, strong passwords (unique per account), and cryptology in communication (i.e., encrypted text messages).

3. Turn on two-factor authentication

Cloud-based websites usually require usernames and passwords. Government agencies need additional information to circumvent this process. One method of further account security is two-factor authentication. This feature utilizes time-based tokens that change every 30 seconds. When activated, two-factor authentication is required after correctly providing username and password credentials. If a password were stolen, the encrypted token would still be necessary.

4. Buy an air-gapped computer
The Electronic Frontier Foundation (EFF; 2014) suggests that with more sensitive information, an air-gapped computer should be used. Air-gapped computers have all Internet capabilities disabled or forcibly removed. The NSA (2010) recommends that Mac users have “an Apple-certified technician remove” wireless cards. For high-risk clients, notes and information would be maintained, but need to be moved via external device (i.e., USB flash drive).

5. Modify informed consent process

The APA Ethics Code (2010) asks that informed consent be given at the outset of treatment. If client and practitioners express an interest in digital technologies to enhance treatment, informed consent should properly explain, justify, and present risks to communication methods (Devereaux & Gottlieb, 2012). If clients express concern during informed consent, and in the interest of autonomy and privacy, practitioners should consider more basic methods (i.e., pen and paper).

Conclusion

Clients (Rubanowitz, 1987; VandeCreek, Miars, & Herzog, 1987) and psychologists have agreed that confidentiality is imperative for provision of care (Donner, VandeCreek, Gonsiorek, & Fisher, 2008; Fisher, 2008; Glosoff et al., 1997). Additionally, the U.S. Supreme Court reasserted psychotherapeutic privilege for client confidentiality in the 1996 case, Jaffee v. Redmond. Despite this historical precedence, government policies have threatened privacy. Each technological innovation provides greater flexibility and accessibility for care. Unfortunately, as Baker and Bufka (2011) suggest, psychologists are engaging with technologies that have legal and ethical ramifications for clients, research participants, and third-party providers. While the APA has created guidelines and standards for interacting with technology,
there are risks to certain communication and storage mediums, especially when using cloud-based providers. Now more than ever, practitioners should be circumspect to new technologies related to the communication and storage of client data. By adopting the best practices listed within this article, practitioners will be taking a stand for client and human rights.
References


Counterintelligence access to telephone toll and transactional records. 18 U.S. Code § 2709.


