

THE TIMES OF ISRAEL | www.timesofisrael.com

This post has been contributed by a third party. The opinions, facts and any media content here are presented solely by the author, and The Times of Israel assumes no responsibility for them. In case of abuse, [report this post](#).

Why you should care about the Panama Papers

DEBORAH HOUSEN-COURIEL | APRIL 12, 2016, 3:23 PM |

Encryption technology – and probably each one of us — is the big winner in last week’s news of [the massive breach into the servers of Mossack Fonseca](#), the Panama-based law firm that had built up a leading global practice since 1977 as a leading creator of shell corporations.

Although not intrinsically illegal, establishment of such corporations can enable the wealthy to stash earnings in order to avoid tax reporting in their home countries, and can blur the “money trail” that lawmakers need to follow while tracing laundered and other illegitimate funds.

Twelve current and former heads of states and another 130 prominent political leaders and public officials have been named in the wide media coverage of the breach, including Russia’s President Putin, President Macri of Argentina, Prime Minister Sharif of Pakistan, and UK Prime Minister David Cameron. Iceland’s Prime Minister Sigmandur David Gunnlaugson already been forced to resign as a result of the leak, after his name was tied to a shell company that he had not declared to tax authorities. Tax and anti-corruption investigations have been opened up in several countries in the wake of the publication of the “Panama Papers,” as the leaked documents have already come to be called, including Israel, Austria, Australia, France, Germany, India, Mexico, the Netherlands, Norway, Sweden and the United States.

The exposure by an anonymous whistleblower is unprecedented: 2.6 terabytes of data in more than 11.5 million documents — PDFs, database files, images and emails. The record-breaking quantity of data leaked in comparison with other notorious hacks is shown graphically in this chart prepared by the German newspaper [Süddeutsche Zeitung](#), the media source originally contacted in 2014 by the still-anonymous whistleblower.

For more than a year prior to publication of the data, media organizations cooperated behind the scenes to analyze Mossack Fonseca’s data to be stored on encrypted drives, also using encrypted communications to manage the logistics of working through the sensitive material while keeping the story from spilling ahead of time. Following exposure of the breach, these millions of documents are being stored in an Amazon cloud data center, where anyone can access them through [the website of the International Consortium of Investigative Journalists](#). Since 2014, the ICIJ has been coordinating an international team of dozens of media organizations, including *Haaretz*, in more than 80 countries. Four hundred journalists have

been sorting through raw data that was originally made available to the *Süddeutsche Zeitung*. That German daily, as well as the ICIJ, maintain that they still do not know the identity of the person or group behind the leak.

Let that sink in: this is far and away the biggest known data breach in history, it was analyzed by 400 journalists worldwide for more than a year, and we don't know who leaked it. How is that possible?

The key to the Mossack Fonseca data exposure was the careful and systematic use of encryption techniques by the anonymous leaker and the journalists he or she contacted. Edward Snowden used similar technology in his exposure of NSA data in 2013, as related by one of his key contacts, journalist Glenn Greenwald, in the 2014 book "No Place to Hide".

Encryption protects data by allowing access only by authorized parties who have been equipped with the relevant decryption tools. The Panama Papers leak embodies the cat-and-mouse dynamic that has long characterized interactions between those who encrypt and those who attempt to decrypt in an unauthorized way.

So on the one hand, the journalists who exposed the Mosseck Fonseca data carefully constructed a well-encrypted operation for the transmission and storage of sensitive data over the course of many months. On the other, they were themselves engaged in the exposure of data that was protected, or was at least intended to be so — there are questions about [the extent to which the company in fact protected its customers' sensitive data](#). Whether this particular breach might be characterized as a "Robin Hood breach" — exposing those who may have broken laws requiring data reporting — the fact remains that the original whistleblower has retained anonymity in order to avoid the consequences of his or her leak of sensitive data.

This anonymity, readily available to any individual or group for communications in cyberspace, is a boon for the protection of the privacy and confidentiality of communications in the face of increasing public awareness of pervasive government surveillance of our communications and data, highlighted by organizations such as the US' [Electronic Frontier Foundation](#). The Economist has also noted the importance of encryption for this [newly-emerging model of global cyber-enabled journalism](#), stating that "The [Panama Papers] affair is ...a triumph for a new model of investigative reporting."

In keeping with this cat-and-mouse development of encryption methods, better tools at many levels of sophistication, confidentiality and price points are continually becoming available to the public for use in our own digital communications. One well-publicized example is [the recent roll-out of end-to-end encryption by the WhatsApp messaging platform](#) to protect its billion users. The recent Apple-FBI standoff over the decryption of information on the iPhone of the San Bernardino terrorist, Syed Farook, has also brought to the fore [the national security and law enforcement implications of encryption technologies](#), and the difficult issues they raise in the context of the elusive balance between privacy and security concerns.

Why is the Panama Papers data breach into the supposedly-protected private bank accounts of the world's rich, famous, and powerful so important for the rest of us? And why is it already a

significant milestone in the fast-developing “data wars” around the issues of privacy and security in cyberspace?

In our new digital environment, developments such as the Panama Papers leak push us to cope with new legal and ethical dilemmas. As beneficial as sophisticated encryption may be for protecting our own digital identities and those of investigative journalists, it is crucial to be fully aware that publicly-available encryption technologies also ensure the anonymity in cyberspace of criminals, terrorists, and other wrongdoers. Both state and non-state actors now leverage the capabilities available for ensuring anonymity on a regular basis. The Panama Papers data breach has also shone a light on the use of encryption technology as a key tool in protecting identities of the rich and mighty who will continue to store funds illegitimately, in shell corporations that are more conscientiously encrypted than those of the Mossack Fonseca unfortunates.

Encryption is good for all of us — but it’s a double-edged sword that will always cut both ways in the delicate balance between the values of privacy protection and those of law enforcement and national security.

Adv. Deborah Housen-Couriel is an Israeli attorney specializing in cybersecurity law and regulation. She works with Konfidas Digital, a Tel Aviv cybersecurity consulting firm, and with Zeichner, Ellman and Krause LLC in New York and Israel. Deborah is also a research fellow at Tel Aviv University’s Interdisciplinary Cyber Research Center and the Herzliya ICT, and a member of the board of Forum Dvora.

YOU MAY LIKE



New German Method Makes Smarter - Do This Daily!

NeuroNation



Gamers around the world have been waiting for this...

Forge Of Empires



How to Trade Step by Step With Jim Cramer

Topdust



Donald Trump's Next Big Challenge: His History With...

InsideSources



Many Retirees Own World's "Most Dangerous Asset"

The Motley Fool



The most addictive game of the year! Build your city!

Forge Of Empires

Recommended by

FROM THE WEB

FROM THE TIMES OF ISRAEL

- Here's the House Obama Will Live in After He Moves Out of the White... (Mansion Global)
- 10 Prettiest Weather Forecast Ladies on TV Worldwide (Sugarmummies)
- 10 Hottest Weather Forecast Women On TV - Check Out! (Sugarmummies)
- Where the World's Billionaires Live (Mansion Global by Dow Jones)
- Top 11 JSON Performance & Usage Tips (Stackify)
- Gamers around the world have been waiting for this game! (Forge Of Empires)
- A sense of direction (Bechukotai, Covenant & Conversation 5776 on...)
- Trump: US must strengthen alliance with Israel
- Egypt: Muslim mob attacks Christians, parades naked woman
- Businessman throws \$2m bar mitzvah for twin sons
- Israel's leaky security barrier a free pass for terror cells
- Jewish philanthropist charged with bribing NYC union leader

Recommended by