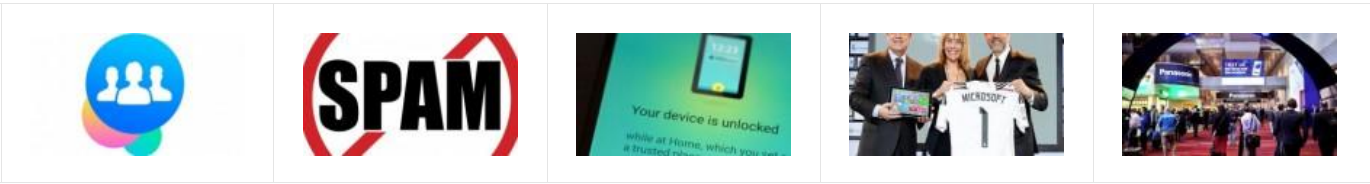
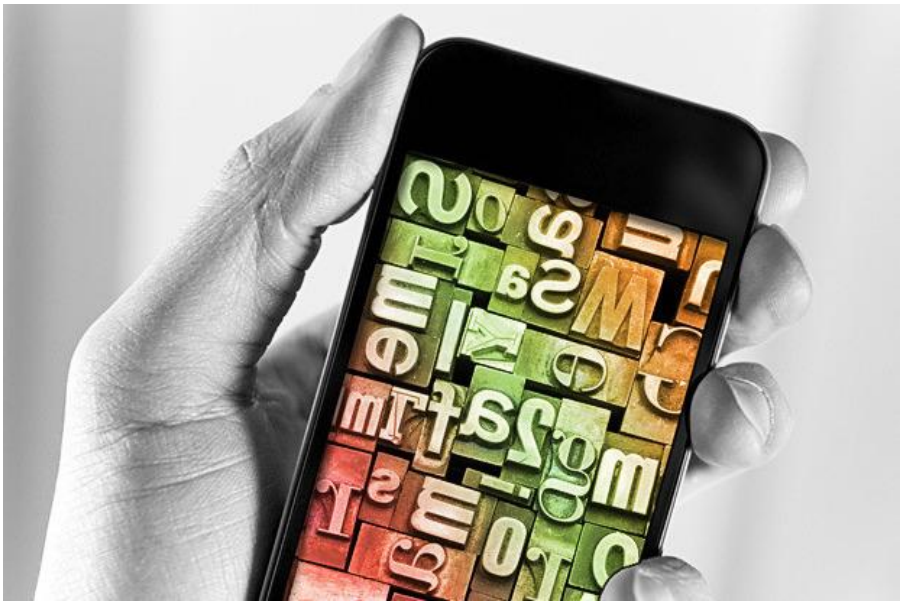


Smartphone Encryption – What Does it Mean to You?

EN CIO CREADO 18 NOVIEMBRE 2014 VISTO: 4 X



Why are legislators considering going to congress for access to our cell phones? What has changed recently to motivate these demands for legislative changes?

The Communications Assistance for Law Enforcement Act, or CALEA, passed in 1994, gave access to our voice communications to wiretap our phone to members of the law enforcement community. This law required all telephone service providers to make it possible for law enforcement to wiretap phones.

The law did not anticipate any of the new technology which is now commonplace. The access is still permissible, but now the data and metadata which used to be accessible are garbled.

The two main cellular operating system (OS) vendors, Apple and Google with their respective iOS and Android operating systems, have recently implemented new security protocols for data storage, which automatically encrypt the information stored on the mobile devices which use these OSs. Both Apple and Google use very sophisticated encryption algorithms, which can take years of processing power to decrypt a single device. Further, neither vendor built a “back door” for access without the user password into their device.

[Online monitoring scheme bad news for security, opponents say]

Unfortunately, we have ample evidence, in both the civil and criminal sectors, that the use of wiretaps has been sorely abused. High profile Los Angeles-based private investigator Anthony Pellicano’s justification for incarceration and the NSA’s well-publicized unwarranted privacy intrusions, and violations of the Fourth Amendment, are two glaring examples of these abuses

The ubiquitous nature of mobile communications today has increased the value of, and potential accessibility to, these conversations

Ciencia
Salud
Hogar
Medio Ambiente
Noticias Insólitas
Tecnología
Cultura
Música
Cine y Tv
Gente - Sociedad
En Familia
Viajes
Estilo
Artes y Letras
Mobiles Tablets Apps
PC Consolas Gadgets
Computer Hoy
Peru.com | Nintendo
Peru.com | Playstation
Peru.com | Xbox
Peru.com | PC
Peru.com | Juegos
Peru.com | Comic
Peru.com | Zona Asia
Peru.com | Extramania
PC World | español
Tecno Magazine
Hobby Consolas
CIO

MÁS LEÍDO EN PC CONSOLAS

(or at least all the data documenting these conversations). We all use our mobile devices with the expectation of privacy, even though we know the transmission medium, the atmosphere, is wide open for interception.

The same is true for information about who we called, how long we spoke and all the details and content of our non-verbal communications. We all have conversations that, if recorded, overheard or viewed as text, could go from embarrassing all the way to admission of criminal guilt.

[6 tips for smartphone privacy and security]

As forensic experts we truly understand the probative value of the data and metadata contained on smartphones. These devices are routinely imaged, preserved and analyzed as part of the discovery process in cases where communications are directly or indirectly related to the underlying issues. The data and metadata automatically stored on smartphones can include entire email chains, geographical locations, contacts, logs of who was texted or called, and a host of other information depending on what apps were installed and used (see “Alternative Keyboard apps: Too risky for your smartphone?”).

Most users would have no idea how to access all this information and/or delete it, so it tends to remain on one’s smartphone indefinitely. Since the recent OS changes , this information remains on these devices but is only accessible with the user’s password; no more going to vendors like Apple with subpoenas and gaining access to a locked iPhone.

A Virginia District court recently ruled that a suspect is not required to give up their password if requested by police, but since detainees do have to provide fingerprints, they can be used to unlock your phone if Touch ID is used instead of a password.

Knowing the potential value of this information, and that access can be denied by the phone owner, is potentially very frustrating to law enforcement and litigators. In civil litigation, this is not as much of an issue, as a judge can threaten the phone owner with contempt of court or sanctions if they do not produce information required for access (this can also work in criminal matters, but with only money at stake these punishments tend to be more effective in civil matters).

“Don’t be lulled into thinking that your personal information is safe from prying eyes.”

Don’t be lulled into thinking that your personal information is safe from prying eyes. If you backup to the cloud or a computer, or periodically sync your smartphone, you may be leaving most, if not all, of the information which is now encrypted on your phone, in an unencrypted state in one or both of those other locations.

So if you are caught up in illegitimate activities, these new OS changes may not be the “get out of jail free card” you were hoping for. You should immediately read “6 tips for smartphone privacy and security” or maybe start using those “burners” Saul in “Breaking Bad” used and routinely handed out to his clients.

Ronald Kaplan, MS, MBA is a partner at SICons, a management consulting and computer forensic expert witness firm in Los Angeles. Dylan Kaplan, BS, is a recent graduate of the Eller College of Management at the University of Arizona, specializing in Management Information Systems. While at the University of Arizona, Dylan worked at Apple Inc. providing technical support. He is currently a systems engineer living in Silicon Valley.

This story, "Smartphone Encryption – What Does it Mean to You?" was originally published by CSO.

Fuente de la noticia: CIO

Leer noticia en el periódico