SB

38

<TARGET><BILL>SB 38</BILL><SUBJECT>SB
38</SUBJECT><COMM>SSTA29</COMM></TARGET>

ALASKA STATE LEGISLATURE

EAU
STATE CAPITOL BLDG. RM 9
JUNEAU, AK 99801-1182
PHONE (907) 465-4930
ALASKASENATEDEMS.COM/GARDNER

ANCHORAGE
716 W. 4TH AVENUE
ANCHORAGE, AK 99501
PHONE (907) 269-0174
FACEBOOK.COM/BERTAGARDNER

SENATOR BERTA GARDNER
SENATE DISTRICT I

Sponsor Statement

SB38 – *"An Act relating to a warrant requirement for searches of electronic devices"*

Alaskans have long recognized the inherent right of privacy, enshrining a protection for it in the state constitution in 1972. In recent years, privacy has taken on new significance as Americans become more and more aware of the intense scrutiny put upon their electronic information.

Security breaches at big names like Target, Home Depot, and Sony coupled with revelations of spying by US and foreign intelligence agencies on their constituencies, has brought with it an important lesson: as we use electronic information to store valuable information, we must be careful in crafting laws that protect our privacy in the context of modern day technologies. Senate Bill 28 is a first step in addressing those concerns in Alaska.

By 2020, 80% of all adults in the US will own a smartphone, *The Economist* reports. Since 2007, when Steve Jobs announced the first Apple iPhone, we've continued to use our smartphones, and the internet generally, for sensitive transactions like banking, tax filing, bill payment, and many others.

With the great potential for a more technologically connected society, comes also heightened fears of privacy. Senate Bill 38 seeks to protect Alaskans' privacy in electronic information by mandating that law enforcement must obtain a warrant before accessing private electronic information.

Reasonable exceptions can be made to this mandate in the event of an emergency, or if the owner agrees to a search prior to a warrant being issued.

In 1972, Alaskans had a very public discussion about privacy in voting on a constitutional amendment to a right to privacy. Although that was discussion took place more than 40 years ago, it is ironic that even then, the concern was over invasion of electronic privacy.

Delegates to the constitutional convention even considered stronger language addressing electronic invasions of privacy, though that idea was later scrapped. Our state has a long history of acknowledging the right to privacy.

SB38 seeks to bring Alaska privacy statutes in line with modern day technologies.

Article 1 - Declaration of Rights

§ 1. Inherent Rights

This constitution is dedicated to the principles that all persons have a natural right to life, liberty, the pursuit of happiness, and the enjoyment of the rewards of their own industry; that all persons are equal and entitled to equal rights, opportunities, and protection under the law; and that all persons have corresponding obligations to the people and to the State.

§ 2. Source of Government

All political power is inherent in the people. All government originates with the people, is founded upon their will only, and is instituted solely for the good of the people as a whole.

§ 3. Civil Rights

No person is to be denied the enjoyment of any civil or political right because of race, color, creed, sex, or national origin. The legislature shall implement this section. [Amended 1972]

§ 4. Freedom of Religion

No law shall be made respecting an establishment of religion, or prohibiting the free exercise thereof.

§ 5. Freedom of Speech

Every person may freely speak, write, and publish on all subjects, being responsible for the abuse of that right.

§ 6. Assembly; Petition

The right of the people peaceably to assemble, and to petition the government shall never be abridged.

§ 7. Due Process

No person shall be deprived of life, liberty, or property, without due process of law. The right of all persons to fair and just treatment in the course of legislative and executive investigations shall not be infringed.

§ 8. Grand Jury

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the armed forces in time of war or public danger. Indictment may be waived by the accused. In that case the prosecution shall be by information. The grand jury shall consist of at least twelve citizens, a majority of whom concurring may return an indictment. The power of grand juries to investigate and make recommendations concerning the public welfare or safety shall never be suspended.

§ 9. Jeopardy and Self-Incrimination

No person shall be put in jeopardy twice for the same offense. No person shall be compelled in any criminal proceeding to be a witness against himself.

§ 10. Treason

Treason against the State consists only in levying war against it, or in adhering to its enemies, giving them aid and comfort. No person shall be convicted of treason, unless on the testimony of two witnesses to the same overt act, or on confession in open court.

§ 11. Rights of Accused

In all criminal prosecutions, the accused shall have the right to a speedy and public trial, by an impartial jury of twelve, except that the legislature may provide for a jury of not more than twelve nor less than six in courts not of record. The accused is entitled to be informed of the nature and cause of the accusation; to be released on bail, except for capital offenses when the proof is evident or the presumption great; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

§ 12. Criminal Administration

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted. Criminal administration shall be based upon the following: the need for protecting the public, community condemnation of the offender, the rights of victims of crimes, restitution from the offender, and the principle of reformation. [Amended 1994]

§ 13. Habeas Corpus

The privilege of the writ of habeas corpus shall not be suspended, unless when in cases of rebellion or actual or imminent invasion, the public safety requires it.

§ 14. Searches and Seizures

The right of the people to be secure in their persons, houses and other property, papers, and effects, against unreasonable searches and seizures, shall not be violated. No warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized.

§ 15. Prohibited State Action

No bill of attainder or ex post facto law shall be passed. No law impairing the obligation of contracts, and no law making any irrevocable grant of special privileges or immunities shall be passed. No conviction shall work corruption of blood or forfeiture of estate.

§ 16. Civil Suits; Trial by Jury

In civil cases where the amount in controversy exceeds two hundred fifty dollars, the right of trial by a jury of twelve is preserved to the same extent as it existed at common law. The legislature may make provision for a verdict by not less than three-fourths of the jury and, in courts not of record, may provide for a jury of not less than six or more than twelve.

§ 17. Imprisonment for Debt

There shall be no imprisonment for debt. This section does not prohibit civil arrest of absconding debtors.

§ 18. Eminent Domain

Private property shall not be taken or damaged for public use without just compensation.

§ 19. Right to Keep and Bear Arms

A well-regulated militia being necessary to the security of a free state, the right of the people to keep and bear arms shall not be infringed. The individual right to keep and bear arms shall not be denied or infringed by the State or a political subdivision of the State. [Amended 1994]

§ 20. Quartering Soldiers

No member of the armed forces shall in time of peace be quartered in any house without the consent of the owner or occupant, or in time of war except as prescribed by law. The military shall be in strict subordination to the civil power.

§ 21. Construction

The enumeration of rights in this constitution shall not impair or deny others retained by the people.

§ 22. Right of Privacy

The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section. [Amended 1972]

§ 23. Resident Preference

This constitution does not prohibit the State from granting preferences, on the basis of Alaska residence, to residents of the State over nonresidents to the extent permitted by the Constitution of the United States. [Amended 1988]

§ 24. Rights of Crime Victims

Crime victims, as defined by law, shall have the following rights as provided by law: the right to be reasonably protected from the accused through the imposition of appropriate bail or conditions of release by the court; the right to confer with the prosecution; the right to be treated with dignity, respect, and fairness during all phases of the criminal and juvenile justice process; the right to timely disposition of the case following the arrest of the accused; the right to obtain information about and be allowed to be present at all criminal or juvenile proceedings where the accused has the right to be present; the right to be allowed to be heard, upon request, at sentencing, before or after conviction or juvenile adjudication, and at any proceeding where the accused's release from custody is considered; the right to restitution from the accused; and the right to be informed, upon request, of the accused's escape or release from custody before or after conviction or juvenile adjudication. [Amended 1994]

§ 25. Marriage

To be valid or recognized in this State, a marriage may exist only between one man and one woman. [Amended 1998]

Return to Alaska Constitution Table of Contents

Constitutional Amendment Summary

1966-2004 Proposed Amendment Titles & Vote Counts

Election Date	Subject of Amendment	Provisions Affected	Resolution Number	Votes For	Votes Against
8/23/66	Residency Requirement to Vote for President	Article V, Section 1	SJR 1 (1966)	36,667	12,383
8/27/68	Commission on Judicial Qualifications	Article IV, Section 10	HJR 74 (1968)	32,481	12,823
8/27/68	Compensation of Judicial Qualification Commission	Article IV, Section 13	HJR 74 (1968)	27,156	17,467
8/25/70	Establish Voting Age at 18 Years	Article V, Section 1	HJR 7 (1969)	36,590	31,216
8/25/70	Remove English Requirement for Voting	Article V, Section 1	HJR 51 (1970)	34,079	32,578
8/25/70	Secretary of State Designated Lieutenant Governor	Article III, Sections7-11, 13-15; Article XI, Sections 2-6; Article XIII, Sections 1,3; Article XV, Section 9	SJR 2 (1970)	46,102	18,781
8/25/70	Chief Justice Elected by Supreme Court	Article IV, Section 2	HJR 11 (1970)	44,055	19,583
8/25/70	Term of Office for Judicial System Administrator	Article IV, Section 16	HJR 11 (1970)	43,462	18,651
8/22/72	Residency Requirement for Voting	Article V, Section 1	HJR 126 (1972)	31,130	20,745
8/22/72	Prohibition of Sexual Discrimination	Article I, Section 3	HJR 102 (1972)	43,281	10,278
8/22/72	Right of Privacy	Article I, Section 22	SJR 68 (1972)	45,539	7,303
8/22/72	Eliminate City Representation on Borough Assemblies	Article X, Section 4	SJR 52 (1972)	30,132	19,354
8/22/72	Authorize Limited Entry Fisheries	Article VIII, Section 15	SJR 10 (1971)	39,837	10,761
8/22/74	Voting on Constitutional Amendments at General Elections	Article XIII, Section 1	HJR 20 (1973)	56,017	20,403
11/02/76	Action on Veto of Bills	Article II, Sections 9 and 16	HJR 11 (1975)	71,829	39,980
11/02/76	Authorize Permanent Fund	Article IX, Sections 7 and 15	HJR 39 (1976)	75,588	38,518
11/02/76	Administration and Review of State Land Disposals	Article VIII, Section 10	SJR 45 (1976)	46,652	64,744
11/02/76	Direct Financial Aid to Students	Article VII, Section 1	HJR 73 (1976)	54,636	64,211
11/07/78	Powers of Legislative Interim Committees	Article II, Section 11	SJR 16 (1978)	48,078	68,403
11/04/80	Legislative Annulment of Regulations	Article II, New Section	HJR 82 (1980)	58,808	82,010
11/04/80	Disqualification of Legislators	Article II, New Section	SJR 2 (1980)	47,054	99,705
	Interim and Special Legislative		HJR 80		

11/04/80	Committees	Article II, Section 11	(1980)	41,868	102,270
11/04/80	Appointment and Confirmation of Members	Article III, Section 26	HJR 20 (1980)	56,316	90,506
11/02/82	Veterans' Housing Bond Authority	Article IX, Section 8	HJR 71 (1982)	111,460	69,497
11/02/82	Changes in Commission on Judicial Qualifications	Article IV, Section 10	HJR 32 (1981)	123,172	53,424
11/02/82	Limiting Appropriation Increases	Article IX, Section 16; Article XV, Sections 26-28	SJR 4 (1981)	110,669	71,531
11/06/84	Legislative Annulment of Administration Regulations	Article II, New Section	HJR 5 (1983)	91,171	98,855
11/06/84	Limit Length of Legislative Session	Article II, Section 8	HJR 2 (1984)	150,999	46,099
11/04/86	Legislative Annulment of Administrative Regulations	Article II, New Section	SJR 40 (1986)	65,176	94,299
11/08/88	Resident Hiring Preference	Article I, Section 23	HJR 18 (1988)	162,997	31,650
11/06/90	Budget Reserve Fund	Article IX, Section 17	SJR 5 (1990)	124,280	63,307
11/08/94	Individual Right to Keep and Bear Arms	Article I, Section 19	SJR 39 (1994)	153,300	57,636
11/08/94	Rights of Crime Victims	Article I, Sections 12, 24	HJR 43 (1994)	178,858	27,641
11/05/96	Voter Approval of Changes to Statehood Act	Article XII, Section 14	SJR 3 (1996)	157,936	71,082
11/03/98	Definition of Marriage	Article I, Section 25	SJR 42 (1998)	152,965	71,631
11/03/98	Redistricting	Article VI, Sections 1-11; Article XI, Section 3; Article XIV, Sections 1-3; Article XV, Section 29	HJR 44 (1998)	110,768	101,686
11/07/00	Prohibition on Wildlife Initiative	Article XI, Section 7	HJR 56 (2000)	96,253	179,552
11/07/00	Amendment Provision; Prohibit Court Intervention	Article XIII, Section 1; New Section	SJR 27 (2000)	114,310	151,467
11/07/00	Confirmation of Board Appointees	Article III, Section 26; Article IX, Section 15	SJR 34 (2000)	72,419	194,975
11/02/04	Requirements for Initiative & Referendum	Article XI, Section 3	HJR 5 (2004)	149,236	139,642

Shading indicates proposed amendment failed.

Return to Alaska Constitution Table of Contents

Alaska's Constitution

A Citizen's Guide

Gordon Harrison

Alaska Legislative Affairs Agency

FIFTH EDITION

The second sentence has no direct counterpart in the U.S. Constitution, but the principle is embodied in the federal provision that the president is the commander and chief of the army and navy (Article II, Section 2). Virtually all state constitutions contain a similar statement, which expresses a basic tenet of democratic government.

Section 21. Construction

> **The enumeration of rights in this constitution shall not impair or deny others retained by the people.**

That Article I may omit mention of some rights does not mean that these rights are surrendered by the people. This provision is common in state constitutions, and it is a principle recognized by Article Nine of the Bill of Rights: "The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people." These provisions have been used very seldom by state or federal courts. In Alaska, it has only been recognized as protecting the right of representing oneself in court proceedings. The Alaska Supreme Court allowed a prisoner to act as his own attorney in post-conviction proceedings, provided that he was capable of presenting his case in a rational and coherent manner, he recognized what he was giving up by declining the assistance of counsel, and he could conduct himself with a minimum of courtroom decorum. "At the time that the Alaska Constitution was enacted and became effective, the right of self-representation was so well established that it must be regarded as a right 'retained by the people'" *(McCracken v. State,* 518 P.2d 85, 1974).

Section 22. Right of Privacy

> **The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.**

This section was added to the constitution by amendment in 1972. It was prompted by fear of the potential for misuse of computerized information systems, which were then in their infancy. Delegates to the constitutional convention 16 years earlier had also been concerned about the potential for technological intrusion in the lives of ordinary citizens, but then the fear was electronic surveillance and wiretapping. They considered, but ultimately rejected, inclusion of the following language in the section dealing with unreasonable searches and seizures: "The right of privacy of the individual shall not be invaded by use of any electronic or other scientific transmitting, listening or sound recording device for the purpose of gathering incriminating evidence. Evidence so obtained shall not be admissible in judicial or legislative hearings."

In the early 1970s, the Alaska Department of Public Safety was developing the Alaska Justice Information System, a computerized database of information on the criminal history of individuals. Fearful that such a system was the precursor of a "Big Brother" government information bureaucracy, legislators responded with this constitutional amendment, which was handily ratified by the voters.

Alaska is one of a small group of states with a constitutional right of privacy: similar provisions can be found in the constitutions of Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington. (Some of these were added by amendment at approximately the same time as Alaska's.) The U.S. Constitution does not contain an explicit right of privacy. However, in recent years the U.S. Supreme Court has ruled that basic privacy rights are inferred from the First, Third, Fourth, Fifth and Ninth Amendments.

Like other basic constitutional rights, the right of privacy is not absolute. Reasonable interferences with privacy are tolerated, as are, for example, reasonable restraints on the right of free speech. To judge the acceptability of government interference with citizens' privacy, the courts use the same balancing test applied in other cases where it is alleged that the state has trampled a person's rights: the more significant the right involved, the more important the state's interest must be in adopting the restrictive law or regulation.

The first major judicial interpretation of the new constitutional right of privacy in Alaska arose from a case not involving electronic intrusion but the use of marijuana in the home. In this landmark case that overturned a state law making it illegal to possess marijuana under any circumstances, the Alaska Supreme Court found privacy in the home to be of the highest importance and the most deserving of constitutional protection, and it found the state's case for regulating the personal use of small amounts of marijuana to be less than compelling *(Ravin v. State,* 537 P.2d 494, 1975). In subsequent cases, however, the court upheld the state laws against the possession of small amounts of marijuana in public (saying the right of personal privacy in public places is of lesser constitutional significance; *Belgarde v. State,* 543 P.2d 206, 1975) and against the possession of small amounts of cocaine in the home (saying the harmful societal effects of cocaine are serious enough to justify the state's regulation of the substance, even in the home; *State v. Erickson,* 574 P.2d 1, 1978). The supreme court upheld a Juneau ordinance that prohibited smoking in private clubs that served food or alcohol. The court said that a club was not an extension of the home, and that the ordinance did not violate the state constitutional right to privacy *(Fraternal Order of Eagles v. City and Borough of Juneau,* 254 P.3d 348, 2011).

Alaska's constitutional right to privacy has also been interpreted to protect a woman's access to an abortion. In 1992, the governing board of a private hospital in the city of Palmer adopted a policy to prohibit abortions in their facility, relying on a state law that said neither a person nor hospital would be liable for refusing to participate in an abortion. A lawsuit successfully contested the board's decision: the Alaska Supreme Court said that the hospital, which was licensed by the state and received substantial amounts of public money, must allow abortions to be performed, and the portion

of the state law upon which the board relied was unconstitutional *(Valley Hospital Association v. Mat-Su Coalition for Choice,* 948 P.2d 963, 1997). In subsequent cases the court ruled that reproductive rights protected by this section extend to minors *(State v. Planned Parenthood of Alaska,* 35 P.3d 30, 2001, and 171 P.3d 577, 2007). At issue in these cases was a 1997 state law requiring a minor to obtain her parent's consent in order to obtain an abortion. The court ruled that the law violated the minor's right of privacy, but suggested that a law simply requiring notification of the minor's parents prior to an abortion would not offend the privacy protections of this section. A law requiring parental notification was adopted by an initiative that appeared on the ballot at the primary election on August 24, 2010. (Another court decision dealing with abortion, which prohibited the state's Medicaid program from denying medically necessary abortions to needy women, was decided on the basis of a violation of the equal protection clause of Section 1 of this article; see *State v. Planned Parenthood of Alaska,* 28 P.3d 904, 2001.*)*

Most privacy cases arise in the context of searches and seizures (see Section 14 above). Of these, a leading case is *State v. Glass* (583 P.2d 872, 1978), in which the Alaska Supreme Court ruled that the state could not use as evidence a recording, made without a warrant, of a conversation between the defendant and an informant who possessed a wireless transmitter. Although the U.S. Supreme Court had ruled that recordings of this type were admissible evidence, the Alaska Supreme Court found that Alaska's constitutional protection was broader than the inferred right of privacy from the federal constitution: "Were that not the case, there would have been no need to amend the constitution." Eighteen years after *Glass*, the court of appeals ruled that a warrantless, surreptitious video recording without sound also violated the right to privacy (*State v. Page,* 911 P.2d 513, Alaska Ct. App., 1996). In these and similar cases the court uses a test enunciated in *Glass* that asks if the defendant had a reasonable expectation of privacy in the place and activity at issue. For example, the court has determined that fishermen do not have a reasonable expectation that catches stored in the holds of their vessels will be protected from warrantless searches *(Dye v. State,* 650 P.2d 418, Alaska Ct. App., 1982). A theater box office employee caught stealing on a hidden surveillance camera did not have a reasonable expectation of privacy selling tickets to the public (*Cowles v. State*, 23 P.3d 1168, 2001).

Section 23. Resident Preference

> **This constitution does not prohibit the State from granting preferences, on the basis of Alaska residence, to residents of the State over nonresidents to the extent permitted by the Constitution of the United States.**

This section of Article I was passed by the legislature and ratified by the voters in 1988. It was intended to prevent the equal protection clause of Article I, Section 1 from becoming a snag in state courts for local hire (also referred to as "Alaska hire") legislation—that is, legislation that would give preference to job applicants who are residents of the state. Efforts by the legislature to impose a local hire law on employers had been repeatedly frustrated in the courts.

28th Legislature(2013-2014)

Bill History/Action for 28th Legislature

BILL: SJR 22 **SHORT TITLE:** OPPOSE WARRANTLESS DATA COLLECTION

BILL VERSION: HCS SJR 22(JUD)

CURRENT STATUS: LEGIS RESOLVE 51 **STATUS DATE:** 08/11/14

SPONSOR(S): SENATOR(S) GIESSEL, Fairclough, Coghill, McGuire, Bishop, Gardner, Dunleavy, Micciche, Wielechowski, Ellis, Dyson, French, Stevens, Kelly, Meyer, Egan, Huggins – 17 Senate
REPRESENTATIVE(S) Kawasaki, Tuck, Keller, Reinbold, Hughes, Millett, Costello, Feige, Isaacson, Guttenberg, LeDoux, Josephson, Seaton, Pruitt
14 - House

TITLE: Opposing the warrantless collection of telephone call data by the National Security Agency.

Bill Number: Search Bills Next Bill

Full Text | Fiscal Notes | Amendments | Minutes and Audio | Documents

Sponsor Statement

Display Committee Action with Bill History

Jrn-Date	Jrn-Page	Action
02/14/14	1639	(S) READ THE FIRST TIME - REFERRALS
02/14/14	1639	(S) JUD
02/14/14	1644	(S) COSPONSOR(S): MCGUIRE, BISHOP, GARDNER, DUNLEAVY, MICCICHE, WIELECHOWSKI, ELLIS
03/10/14	1910	(S) JUD RPT 3DP
03/10/14	1910	(S) DP: COGHILL, OLSON, DYSON
03/10/14	1910	(S) FN1: ZERO(S.JUD)
03/31/14	2224	(S) RULES TO CALENDAR 3/31/2014
03/31/14	2224	(S) READ THE SECOND TIME
03/31/14	2224	(S) AM NO 1 ADOPTED UNAN CONSENT
03/31/14	2224	(S) ADVANCED TO THIRD READING UNAN CONSENT
03/31/14	2224	(S) READ THE THIRD TIME SJR 22 AM
03/31/14	2224	(S) COSPONSOR(S): DYSON, FRENCH, STEVENS, KELLY, MEYER,
03/31/14	2224	(S) EGAN, HUGGINS
03/31/14	2224	(S) PASSED Y18 N- E2
03/31/14	2228	(S) TRANSMITTED TO (H)
03/31/14	2228	(S) VERSION: SJR 22 AM
04/01/14	2117	(H) READ THE FIRST TIME - REFERRALS
04/01/14	2117	(H) JUD
04/01/14	2134	(H) CROSS SPONSOR(S): KAWASAKI, TUCK, KELLER
04/13/14	2395	(H) JUD RPT HCS(JUD) 5DP
04/13/14	2395	(H) DP: LEDOUX, PRUITT, GRUENBERG, LYNN, KELLER
04/13/14	2395	(H) FN1: ZERO(S.JUD)
04/18/14	2612	(H) RULES TO 1ST SUP CALENDAR 4/18/2014
04/18/14	2612	(H) READ THE SECOND TIME
04/18/14	2612	(H) JUD HCS ADOPTED UNAN CONSENT
04/18/14	2612	(H) ADVANCED TO THIRD READING UNAN CONSENT
04/18/14	2613	(H) READ THE THIRD TIME HCS SJR 22(JUD)
04/18/14	2613	(H) PASSED Y38 E1 A1
04/18/14	2617	(H) CROSS SPONSOR(S): REINBOLD, HUGHES, MILLETT, COSTELLO, FEIGE, ISAACSON,
04/18/14	2617	(H) GUTTENBERG, LEDOUX, JOSEPHSON, SEATON, PRUITT

04/18/14	2619	(H) TRANSMITTED TO (S) AS AMENDED
04/18/14	2619	(H) VERSION: HCS SJR 22(JUD)
04/19/14	2602	(S) CONCUR MESSAGE READ
04/19/14	2603	(S) CONCUR AM OF (H) Y20 N-
09/19/14	2828	(S) 9:25 AM 7/2 TRANSMITTED TO GOVERNOR
09/19/14	2892	(S) PERMANENTLY FILED 8/11 LEGIS RESOLVE 51

Similar Subject Match or Exact Subject Match
COMMUNICATIONS
CONSTITUTION
COURTS
DATA PROCESSING
INTERGOVERNMENTAL RELATIONS
PRIVACY
RIGHTS
TERRORISM

Bill Number: Display Bill
Next Bill

Return to Basis Main Menu (28th Legislature)

STATE OF ALASKA
THE LEGISLATURE

2014

Source
HCS SJR 22(JUD)

Legislative Resolve No.
51

Opposing the warrantless collection of telephone call data by the National Security Agency.

BE IT RESOLVED BY THE LEGISLATURE OF THE STATE OF ALASKA:

WHEREAS the Fourth Amendment to the Constitution of the United States provides "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"; and

WHEREAS the Fifth Amendment to the Constitution of the United States provides "No person shall . . . be deprived of life, liberty, or property, without due process of law"; and

WHEREAS, on December 16, 2013, United States District Court Judge Richard Leon ruled that the National Security Agency's program, bulk collection, and querying of telephone record metadata are likely unconstitutional; and

WHEREAS the legislature objects to the dragnet approach to data collection allowed by the Foreign Intelligence Surveillance Court, a court that operates in secret and, under sec. 215 of the USA PATRIOT Act, issues orders that perpetuate the warrantless collection of data

of nearly all Americans; and

WHEREAS the National Security Agency stores the date and time of calls, their duration, and the participating telephone numbers of the calls of nearly all Americans in a centralized database, which allows National Security Agency analysts to access not only those numbers, but the numbers with which the numbers have been in contact, and, in turn, the numbers in contact with those numbers; and

WHEREAS the Privacy and Civil Liberties Oversight Board, in its January 2014 report titled "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," questions the legal basis for the National Security Agency's mass telephone call data collection program; and

WHEREAS, when telephone call data of Americans is collected by the National Security Agency, that data is not related to specific investigations of the Federal Bureau of Investigation; and

WHEREAS orders issued by the Foreign Intelligence Surveillance Court at the request of the federal government require telephone companies to provide new calling records on a daily basis, a mandate not grounded in statute; and

WHEREAS sec. 215 of the USA PATRIOT Act is designed to enable the Federal Bureau of Investigation to obtain records in the course of investigations, but the National Security Agency's mass collection of the records is not consistent with that design; and

WHEREAS the Electronic Communications Privacy Act of 1986 prohibits telephone companies from sharing consumer data with the government except in special circumstances, and the Privacy and Civil Liberties Oversight Board concluded that the National Security Agency's telephone call data collection program may violate the Act; and

WHEREAS the Privacy and Civil Liberties Oversight Board found that the National Security Agency's telephone call data collection program has not prevented, discovered, or identified terrorist attacks, plots, or suspects that threatened the security of the United States; and

WHEREAS the widespread collection of telephone call data of Americans reveals highly sensitive personal information; and

WHEREAS the legislature resolutely opposes the continuation of the National

Security Agency's warrantless data collection program; and

WHEREAS the legislature views the National Security Agency's storage in a central database of the telephone call metadata of all Americans as an unconstitutional practice that should be immediately suspended; and

WHEREAS the history of government coercion, persecution, and abuse of personal information and human life in the twentieth century prompts the legislature to seek to protect the liberty of future generations from an oppressive and tyrannical federal government; and

WHEREAS the fundamental rights of Americans to speak freely and associate with others are threatened and are likely being diminished by the National Security Agency's mass collection of telephone call data; and

WHEREAS the National Security Agency's mass collection of telephone call data may intimidate or chill the freedom of expression of individuals and groups that disagree with certain government policies or result in extreme scrutiny of those persons simply for opposing those policies; and

WHEREAS the Foreign Intelligence Surveillance Court has deviated from its purpose to authorize warrants for electronic surveillance relating only to a specific person, a specific place, or a specific communications account or device; and

WHEREAS the Foreign Intelligence Surveillance Court operates in a secretive manner that prevents the court from hearing public input regarding government requests to conduct surveillance;

BE IT RESOLVED that the Alaska State Legislature urges the federal government to end the mass telephone call data collection program conducted under sec. 215 of the USA PATRIOT Act, because of its lack of a statutory foundation and because it raises serious constitutional concerns under the Fourth and Fifth Amendments to the Constitution of the United States; and be it

FURTHER RESOLVED that the Alaska State Legislature urges the federal government to eliminate all stored metadata upon ending the mass telephone call data collection program; and be it

FURTHER RESOLVED that the Alaska State Legislature urges the United States Congress to authorize the creation of a panel of private sector lawyers to serve as advocates for the public before the Foreign Intelligence Surveillance Court to increase public knowledge

and oversight; and be it

FURTHER RESOLVED that the Alaska State Legislature urges judges of the Foreign Intelligence Surveillance Court to write opinions in a manner that allows the government to declassify and release the opinions to the public; and be it

FURTHER RESOLVED that the Alaska State Legislature urges the Foreign Intelligence Surveillance Court to work to declassify past opinions and release those opinions to the public; and be it

FURTHER RESOLVED that the Alaska State Legislature requests the United States Attorney General and members of the intelligence and judiciary committees of the United States Congress to inform the Alaska State Legislature of the federal government's activities under the Foreign Intelligence Surveillance Act and provide the Alaska State Legislature with copies of reports submitted under the Foreign Intelligence Surveillance Act; and be it

FURTHER RESOLVED that the Alaska State Legislature urges the Governor to prohibit the use of state personnel and resources to assist the National Security Agency in its collection of mass data on Alaskans without a specific search warrant; and be it

FURTHER RESOLVED that the Alaska State Legislature considers the National Security Agency's unilateral collection of the telephone call data of all Americans a violation of statute, an unconstitutional program, and a troubling overreach by the federal government; the Alaska State Legislature has sworn to uphold both the Constitution of the United States and the Constitution of the State of Alaska and will not assist the federal government by facilitating programs that are tyrannical in nature, that subject Americans to unreasonable and unwarranted searches, and that violate the fundamental principle of liberty; let this resolution serve as a notice to this Administration and all future Administrations that Alaskans reject surrendering their liberty in the name of an unconstitutional program.

COPIES of this resolution shall be sent to the Honorable Barack Obama, President of the United States; the Honorable Joseph R. Biden, Jr., Vice-President of the United States and President of the U.S. Senate; the Honorable John Boehner, Speaker of the U.S. House of Representatives; the Honorable Harry Reid, Majority Leader of the U.S. Senate; the Honorable Patrick J. Leahy, President pro tempore of the U.S. Senate; the Honorable Dianne Feinstein, Chair, U.S. Senate Select Committee on Intelligence; the Honorable Saxby Chambliss, Vice Chair, U.S. Senate Select Committee on Intelligence; the Honorable Mike

Rogers, Chair, U.S. House of Representatives Permanent Select Committee on Intelligence; the Honorable C. A. Dutch Ruppersburger, Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence; the Honorable Jeh Johnson, United States Secretary of Homeland Security; the Honorable Sean Parnell, Governor of Alaska; General Keith B. Alexander, United States Army, Director, National Security Agency; Richard H. Ledgett, Jr., Deputy Director, National Security Agency; James B. Comey, Director, Federal Bureau of Investigation; and the Honorable Lisa Murkowski and the Honorable Mark Begich, U.S. Senators, and the Honorable Don Young, U.S. Representative, members of the Alaska delegation in Congress.

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

RILEY *v.* CALIFORNIA

CERTIORARI TO THE COURT OF APPEAL OF CALIFORNIA, FOURTH APPELLATE DISTRICT, DIVISION ONE

No. 13–132. Argued April 29, 2014—Decided June 25, 2014*

In No. 13–132, petitioner Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pants pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed.

In No. 13–212, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person and noticed that the phone was receiving multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they suspected was Wurie's apartment. They secured a search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment. The District Court denied the motion, and Wurie was convicted. The

---

*Together with No. 13–212, *United States* v. *Wurie*, on certiorari to the United States Court of Appeals for the First Circuit.

Syllabus

First Circuit reversed the denial of the motion to suppress and vacated the relevant convictions.

Held: The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. Pp. 5–28.

(a) A warrantless search is reasonable only if it falls within a specific exception to the Fourth Amendment's warrant requirement. See *Kentucky* v. *King*, 563 U. S. ___, ___. The well-established exception at issue here applies when a warrantless search is conducted incident to a lawful arrest.

Three related precedents govern the extent to which officers may search property found on or near an arrestee. *Chimel* v. *California*, 395 U. S. 752, requires that a search incident to arrest be limited to the area within the arrestee's immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction. In *United States* v. *Robinson*, 414 U. S. 218, the Court applied the *Chimel* analysis to a search of a cigarette pack found on the arrestee's person. It held that the risks identified in *Chimel* are present in all custodial arrests, 414 U. S., at 235, even when there is no specific concern about the loss of evidence or the threat to officers in a particular case, *id.*, at 236. The trilogy concludes with *Arizona* v. *Gant*, 556 U. S. 332, which permits searches of a car where the arrestee is unsecured and within reaching distance of the passenger compartment, or where it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle, *id.*, at 343. Pp. 5–8.

(b) The Court declines to extend *Robinson*'s categorical rule to searches of data stored on cell phones. Absent more precise guidance from the founding era, the Court generally determines whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming* v. *Houghton*, 526 U. S. 295, 300. That balance of interests supported the search incident to arrest exception in *Robinson*. But a search of digital information on a cell phone does not further the government interests identified in *Chimel*, and implicates substantially greater individual privacy interests than a brief physical search. Pp. 8–22.

(1) The digital data stored on cell phones does not present either *Chimel* risk. Pp. 10–15.

(i) Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Officers may examine the phone's physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. To the extent that a search of cell phone data

might warn officers of an impending danger, *e.g.*, that the arrestee's confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances. See, *e.g.*, *Warden, Md. Penitentiary* v. *Hayden*, 387 U. S. 294, 298–299. Pp. 10–12.

(ii) The United States and California raise concerns about the destruction of evidence, arguing that, even if the cell phone is physically secure, information on the cell phone remains vulnerable to remote wiping and data encryption. As an initial matter, those broad concerns are distinct from *Chimel*'s focus on a defendant who responds to arrest by trying to conceal or destroy evidence within his reach. The briefing also gives little indication that either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution. And, at least as to remote wiping, law enforcement currently has some technologies of its own for combatting the loss of evidence. Finally, law enforcement's remaining concerns in a particular case might be addressed by responding in a targeted manner to urgent threats of remote wiping, see *Missouri* v. *McNeely*, 569 U. S. ___, ___, or by taking action to disable a phone's locking mechanism in order to secure the scene, see *Illinois* v. *McArthur*, 531 U. S. 326, 331–333. Pp. 12–15.

(2) A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but more substantial privacy interests are at stake when digital data is involved. Pp. 15–22.

(i) Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives. Pp. 17–21.

Syllabus

(ii) The scope of the privacy interests at stake is further complicated by the fact that the data viewed on many modern cell phones may in fact be stored on a remote server. Thus, a search may extend well beyond papers and effects in the physical proximity of an arrestee, a concern that the United States recognizes but cannot definitively foreclose. Pp. 21–22.

(c) Fallback options offered by the United States and California are flawed and contravene this Court's general preference to provide clear guidance to law enforcement through categorical rules. See *Michigan* v. *Summers*, 452 U. S. 692, 705, n. 19. One possible rule is to import the *Gant* standard from the vehicle context and allow a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest. That proposal is not appropriate in this context, and would prove no practical limit at all when it comes to cell phone searches. Another possible rule is to restrict the scope of a cell phone search to information relevant to the crime, the arrestee's identity, or officer safety. That proposal would again impose few meaningful constraints on officers. Finally, California suggests an analogue rule, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. That proposal would allow law enforcement to search a broad range of items contained on a phone even though people would be unlikely to carry such a variety of information in physical form, and would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Pp. 22–25.

(d) It is true that this decision will have some impact on the ability of law enforcement to combat crime. But the Court's holding is not that the information on a cell phone is immune from search; it is that a warrant is generally required before a search. The warrant requirement is an important component of the Court's Fourth Amendment jurisprudence, and warrants may be obtained with increasing efficiency. In addition, although the search incident to arrest exception does not apply to cell phones, the continued availability of the exigent circumstances exception may give law enforcement a justification for a warrantless search in particular cases. Pp. 25–27.

No. 13–132, reversed and remanded; No. 13–212, 728 F. 3d 1, affirmed.

ROBERTS, C. J., delivered the opinion of the Court, in which SCALIA, KENNEDY, THOMAS, GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. ALITO, J., filed an opinion concurring in part and concurring in the judgment.

Police Use of Cell Phone Surveillance Technology

Cell phones, the information they contain, and the location data they transmit can significantly aid police during investigations. State and federal decision-makers have weighed in on the appropriate police use of cellular information. On June 25, 2014, the United States Supreme Court ruled in *Riley v. California* that warrants are generally required before police can search the contents of an arrestee's cell phone. In addition, at least 10 states have enacted warrant requirements for police before they are able to acquire location or stored data from cellular devices or telecommunication companies.

States With Police Cell Phone Surveillance Laws

Under certain emergency situations law enforcement is able to collect information from cell phones, or obtain location data without first procuring a warrant. Under Indiana and Virginia law, if a police officer obtains location data based on exigent circumstances, they must obtain a court order within 72 of their initial use of the tracking device.

Reporting Requirements - Minnesota's law requires that each request for a warrant for location data be reported to and tracked by the state court administrator. The information collected by the state court administrator must include whether the warrant application was accepted or denied, the time period of its authorization, the nature of the monitoring and the identity of the police officer or agency requesting the warrant. This information is required to be reported to the Legislature biannually.

Notification Requirements - Utah's law requires police who obtain a warrant for location data to notify the owner of the targeted electronic device within 14 days of the conclusion of the operation. Law enforcement must notify the owner that a warrant was issued, of the time period for which data was collected and of the alleged offense.

Enhanced Protections for Journalists - In Indiana, when police request a warrant for location data for a member of the media, the journalist or news entity targeted must be given notice of the request and the ability to be heard in court concerning the issuance of the warrant. Police are not required to notify journalists if they are the target of a criminal investigation and notifying them would pose a risk to the integrity of the investigation.

References:

Police use of UAS Enactments: Alaska HB 255 (2014), Florida SB 92 (2013), Idaho SB 1134 (2013), Illinois SB 1587 (2013), Illinois SB 2937 (2014), Iowa HF 2289 (2014), Indiana HB 1009 (2014), Montana SB 196 (2013), North Carolina SB 402 (2013), Oregon HB 2710 (2013), Tennessee SB 796 (2013), Texas HB 912 (2013), Utah SB 167 (2014), Virginia HB 2012 and SB 1331 (2013), Wisconsin SB 196 (2014).

Police use of Cell Phone Surveillance Enactments: Colorado SB 193 (2014), Indiana HB 1384 (2014), Indiana HB 1009 (2014), Maine SP 484 (2013), Maine SP 157 (2013), Maryland SB 698 (2014), Minnesota SF 2466 (2014), Montana HB 603 (2013), Tennessee SB 2087 (2014), Utah HB 128 (2014), Virginia HB 17 (2014), Wisconsin AB 536 (2014).

The New York Times | http://nyti.ms/1qJ2Wjj

POLITICS

Major Ruling Shields Privacy of Cellphones

Supreme Court Says Phones Can't Be Searched Without a Warrant

By ADAM LIPTAK JUNE 25, 2014

WASHINGTON — In a sweeping victory for privacy rights in the digital age, the Supreme Court on Wednesday unanimously ruled that the police need warrants to search the cellphones of people they arrest.

While the decision will offer protection to the 12 million people arrested every year, many for minor crimes, its impact will most likely be much broader. The ruling almost certainly also applies to searches of tablet and laptop computers, and its reasoning may apply to searches of homes and businesses and of information held by third parties like phone companies.

"This is a bold opinion," said Orin S. Kerr, a law professor at George Washington University. "It is the first computer-search case, and it says we are in a new digital age. You can't apply the old rules anymore."

Chief Justice John G. Roberts Jr., writing for the court, was keenly alert to the central role that cellphones play in contemporary life. They are, he said, "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."

But he added that old principles required that their contents be protected from routine searches. One of the driving forces behind the American Revolution, Chief Justice Roberts wrote, was revulsion against "general warrants," which "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."

"The fact that technology now allows an individual to carry such information in his hand," the chief justice also wrote, "does not make the

information any less worthy of the protection for which the founders fought."

The government has been on a surprising losing streak in cases involving the use of new technologies by the police. In Wednesday's case and in a 2012 decision concerning GPS devices, the Supreme Court's precedents had supported the government. "But the government got zero votes in those two cases," Professor Kerr said.

The courts have long allowed warrantless searches in connection with arrests, saying they are justified by the need to protect police officers and to prevent the destruction of evidence.

But Chief Justice Roberts said neither justification made much sense in the context of cellphones. While the police may examine a cellphone to see if it contains, say, a razor blade, he wrote, "once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one."

The possibility that evidence could be destroyed or hidden by "remote wiping" or encryption programs, Chief Justice Roberts wrote, was remote, speculative and capable of being addressed. The police may turn off a phone, remove its battery or place it in a bag made of aluminum foil.

Should the police confront an authentic "now or never" situation, the chief justice wrote, they may well be entitled to search the phone under a separate strand of Fourth Amendment law, one concerning "exigent circumstances."

On the other side of the balance, Chief Justice Roberts said, is the data contained on typical cellphones. Ninety percent of Americans have them, he wrote, and they contain "a digital record of nearly every aspect of their lives — from the mundane to the intimate."

He wrote, "According to one poll, nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12 percent admitting that they even use their phones in the shower."

Even the word cellphone is a misnomer, he said. "They could just as easily be called cameras, video players, Rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers," he wrote.

Chief Justice Roberts acknowledged that the decision would make law

enforcement more difficult.

"Cellphones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals," he wrote. "Privacy comes at a cost."

But other technologies, he said, can make it easier for the police to obtain warrants. Using email and iPads, the chief justice wrote, officers can sometimes have a warrant in hand in 15 minutes.

Ellen Canale, a spokeswoman for the Justice Department, said the department would work with its law enforcement agencies to ensure full compliance with the decision.

The Supreme Court is occasionally criticized for its lack of technological savvy, but Chief Justice Roberts, 59, seemed fully familiar with what smartphones can do. "The average smartphone user has installed 33 apps," he wrote, "which together can form a revealing montage of the user's life."

There are mobile applications, he said, for "Democratic Party news and Republican Party news," for "alcohol, drug and gambling addictions," for "sharing prayer requests" and for "tracking pregnancy symptoms." Records from those applications, he added, "may be accessible on the phone indefinitely." And yet more information, he said, may be available through cloud computing.

"An Internet search and browsing history," he wrote, "can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cellphone can also reveal where a person has been. Historic location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."

The court heard arguments in April in two cases on the issue, but issued a single decision.

The first case, Riley v. California, No. 13-132, arose from the arrest of David L. Riley, who was pulled over in San Diego in 2009 for having an

The Economist

Smartphones

Planet of the phones

The smartphone is ubiquitous, addictive and transformative

Feb 28th 2015 | From the print edition

THE dawn of the planet of the smartphones came in January 2007, when Steve Jobs, Apple's chief executive, in front of a rapt audience of Apple acolytes, brandished a slab of plastic, metal and silicon not much bigger than a Kit Kat. "This will change everything," he promised. For once there was no hyperbole. Just eight years later Apple's iPhone exemplifies the early 21st century's defining technology.

Smartphones matter partly because of their ubiquity. They have become the fastest-selling gadgets in history, outstripping the growth of the simple mobile phones that preceded them. They outsell personal computers four to one. Today about half the adult population owns a smartphone; by 2020, 80% will. Smartphones have also penetrated every aspect of daily life. The average American is buried in one for over two hours every day. Asked which media they would miss most, British teenagers pick mobile devices over TV sets, PCs and games consoles. Nearly 80% of smartphone-owners check messages, news or other services within 15 minutes of getting up. About 10% admit to having used the gadget during sex.

The bedroom is just the beginning. Smartphones are more than a convenient route online, rather as cars are more than engines on wheels and clocks are not merely a means to count the hours. Much as the car and the clock did in their time, so today the smartphone is poised to enrich lives, reshape entire industries and transform societies—and in ways that Snapchatting teenagers cannot begin to imagine.

Phono sapiens

The transformative power of smartphones comes from their size and connectivity. Size makes them the first truly personal computers. The phone takes the processing power of yesterday's

supercomputers—even the most basic model has access to more number-crunching capacity than NASA had when it put men on the Moon in 1969—and applies it to ordinary human interactions (see article (http://www.economist.com/news/briefing/21645131-smartphone-defining-technology-age-truly-personal-computer)). Because transmitting data is cheap this power is available on the move. Since 2005 the cost of delivering one megabyte wirelessly has dropped from $8 to a few cents. It is still falling. The boring old PC sitting on your desk does not know much about you. But phones travel around with you—they know where you are, what websites you visit, whom you talk to, even how healthy you are.

The combination of size and connectivity means that this knowledge can be shared and aggregated, bridging the realms of bits and atoms in ways that are both professional and personal. Uber connects available drivers to nearby fares at cheaper prices; Tinder puts people in touch with potential dates. In future, your phone might recommend a career change or book a doctor's appointment to treat your heart murmur before you know anything is amiss.

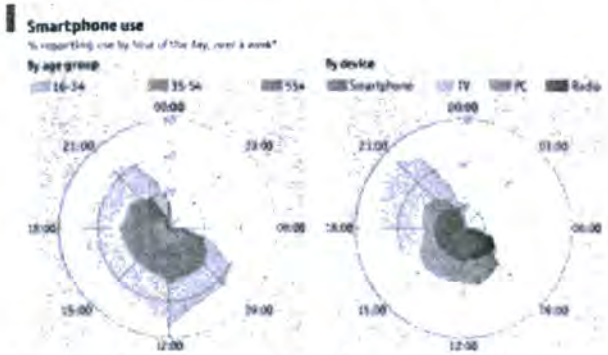
As with all technologies, this future conjures up a host of worries. Some, such as "text neck" (hunching over a smartphone stresses the spine) are surely transient. Others, such as dependency—smartphone users exhibit "nomophobia" when they happen to find themselves empty-handed—are a measure of utility as much as addiction. After all, people also hate to be without their wheels or their watch.

The greater fear is over privacy. The smartphone turns the person next to you into a potential publisher of your most private or embarrassing moments. Many app vendors, who know a great deal about you, sell data without proper disclosure; mobile-privacy policies routinely rival "Hamlet" for length. And if leaked documents are correct, GCHQ, Britain's signals-intelligence agency, has managed to hack a big vendor of SIM cards in order to be able to listen in to people's calls (see article (http://www.economist.com/news/briefing/21645130-watch-out-hackersand-spooks-spy-your-pocket)). If spooks in democracies are doing this sort of thing, you can be sure that those in authoritarian regimes will, too. Smartphones will give dictators unprecedented scope to spy on and corral their unwilling subjects.

The naked app

Yet three benefits weigh against these threats to privacy. For a start, the autocrats will not have it all their own way. Smartphones are the vehicle for bringing billions more people online. The cheapest of them now sell for less than $40, and prices are likely to fall even further. The same phones that allow governments to spy on their citizens also record the brutality of officials and spread information and dissenting opinions. They feed the demand for autonomy and help protest movements to coalesce. A device that hands so much power to the individual has the potential to challenge authoritarianism.

The second benefit is all those personal data which companies are so keen on. Conventional social sciences have been hampered by the limited data sets they could collect. Smartphones are digital census-takers, creating a more detailed view of society than has ever existed before and doing so in real time. Governed by suitable regulations, anonymised personal data can be used, among many other things, to optimise traffic flows, prevent crime and fight epidemics.



Measuring screen time, by age group and device type
(http://www.economist.com/blogs/graphicdetail/2015/02/daily-chart-19)

The third windfall is economic. Some studies find that in developing countries every ten extra mobile phones per 100 people increase the rate of growth of GDP-per-person by more than one percentage point—by, say, drawing people into the banking system. Smartphones will remake entire industries, at unheard-of speed. Uber is a household name, operating in 55 countries, but has yet to celebrate its fifth birthday. WhatsApp was founded in 2009, and already handles 10 billion more messages a day than the SMS global text-messaging system. The phone is a platform, so startups can cheaply create an app to test an idea—and then rapidly go global if people like it. That is why it will unleash creativity on a planetary scale.

By their nature, seminal technologies ask hard questions of society, especially as people adapt to them. Smartphones are no different. If citizens aren't protected from prying eyes, some will suffer and others turn their backs. Societies will have to develop new norms and companies learn how to balance privacy and profit. Governments will have to define what is acceptable. But in eight short years smartphones have changed the world—and they have hardly begun.

From the print edition: Leaders

THE GREAT SIM HEIST

HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE

BY JEREMY SCAHILL AND JOSH BEGLEY @jeremyscahill @joshbegley

02/19/2015

AMERICAN AND BRITISH spies hacked into the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden.

The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

The company targeted by the intelligence agencies, Gemalto, is a multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards. Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world. The company operates in 85 countries and has more than 40 manufacturing facilities. One of its three global headquarters is in Austin, Texas and it has a large factory in Pennsylvania.

In all, Gemalto produces some 2 billion SIM cards a year. Its motto is "Security to be Free."

With these stolen encryption keys, intelligence agencies can monitor mobile communications without seeking or receiving approval from telecom companies and foreign governments. Possessing the keys also sidesteps the need to get a warrant or a wiretap, while leaving no trace on the wireless provider's network that the communications were intercepted. Bulk key theft additionally enables the intelligence agencies to unlock any previously encrypted communications they had already intercepted, but did not yet have the ability to decrypt.

As part of the covert operations against Gemalto, spies from GCHQ — with support from the NSA — mined the private communications of unwitting engineers and other company employees in multiple countries.

Gemalto was totally oblivious to the penetration of its systems — and the spying on its employees. "I'm disturbed, quite concerned that this has happened," Paul Beverly, a Gemalto executive vice president, told *The Intercept*. "The most important thing for me is to understand exactly how this was done, so we can take every measure to ensure that it doesn't happen again, and also to make sure that there's no impact on the telecom operators that we have served in a very trusted manner for many years. What I want to understand is what sort of ramifications it has, or could have, on any of our customers." He added that "the most important thing for us now is to understand the degree" of the breach.

Leading privacy advocates and security experts say that the theft of encryption keys from major wireless network providers is tantamount to a thief obtaining the master ring of a building superintendent who holds the keys to every apartment. "Once you have the keys, decrypting traffic is trivial," says Christopher Soghoian, the principal technologist for the American Civil Liberties Union. "The news of this key theft will send a shock wave through the security community."

> ***THE MASSIVE KEY THEFT IS "BAD NEWS FOR PHONE SECURITY. REALLY BAD NEWS."***

Beverly said that after being contacted by *The Intercept*, Gemalto's internal security team began on Wednesday to investigate how their system was penetrated and could find no trace of the hacks. When asked if the NSA or GCHQ had ever requested access to Gemalto-manufactured encryption keys, Beverly said, "I am totally unaware. To the best of my knowledge, no."

According to one secret GCHQ slide, the British intelligence agency penetrated Gemalto's internal networks, planting malware on several computers, giving GCHQ secret access. We "believe we have their entire network," the slide's author boasted about the operation against Gemalto.

Additionally, the spy agency targeted unnamed cellular companies' core networks, giving it access to "sales staff machines for customer information and network engineers machines for network maps." GCHQ also claimed the ability to manipulate the billing servers of cell companies to "suppress" charges in an effort to conceal the spy agency's secret actions against an individual's phone. Most significantly, GCHQ also penetrated "authentication servers," allowing it to decrypt data and voice communications between a targeted individual's phone and his or her telecom provider's network. A note accompanying the slide asserted that the spy agency was "very happy with the data so far and [was] working through the vast quantity of product."

The Mobile Handset Exploitation Team (MHET), whose existence has never before been disclosed, was formed in April 2010 to target vulnerabilities in cellphones. One of its main missions was to covertly penetrate computer networks of corporations that manufacture SIM cards, as well as those of wireless network providers. The team included operatives from both GCHQ and the NSA.

While the FBI and other U.S. agencies can obtain court orders compelling U.S.-based telecom companies to allow them to wiretap or intercept the communications of their customers, on the international front this type of data collection is much more challenging. Unless a foreign telecom or foreign government grants access to their citizens' data to a U.S. intelligence agency, the NSA or CIA would have to hack into the network or specifically target the user's device for a more risky "active" form of surveillance that could be detected by sophisticated targets. Moreover, foreign intelligence agencies would not allow U.S. or U.K. spy agencies access to the mobile communications of their heads of state or other government officials.

"It's unbelievable. Unbelievable," said Gerard Schouw, a member of the Dutch Parliament, when told of the spy agencies' actions. Schouw, the intelligence spokesperson for D66, the largest opposition party in the Netherlands, told *The Intercept*, "We don't want to have the secret services from other countries doing things like this." Schouw added that he and other lawmakers will ask the Dutch government to provide an official explanation and to clarify whether the country's intelligence services were aware of the targeting of Gemalto, whose official headquarters is in Amsterdam.

Last November, the Dutch government proposed an amendment to its constitution to include explicit protection for the privacy of digital communications, including those made on mobile devices. "We have, in the Netherlands, a law on the [activities] of secret services. And hacking is not allowed," Schouw said. Under Dutch law, the interior minister would have to sign off on such operations by foreign governments' intelligence agencies. "I don't believe that he has given his permission for these kind of actions."

The U.S. and British intelligence agencies pulled off the encryption key heist in great stealth, giving them the ability to intercept and decrypt communications without alerting the wireless network provider, the foreign government or the individual user that they have been targeted. "Gaining access to a database of keys is pretty much game over for cellular encryption," says Matthew Green, a cryptography specialist at the Johns Hopkins Information Security Institute. The massive key theft is "bad news for phone security. Really bad news."

AS CONSUMERS BEGAN to adopt cellular phones en masse in the mid-1990s, there were no effective privacy protections in place. Anyone could buy a cheap device from RadioShack capable of intercepting calls placed on mobile phones. The shift from analog to digital networks introduced basic encryption technology, though it was still crackable by tech savvy computer science graduate students, as well as the FBI and other law enforcement agencies, using readily available equipment.

Today, second-generation (2G) phone technology, which relies on a deeply flawed encryption system, remains the dominant platform globally, though U.S. and European cellphone companies now use 3G, 4G and LTE technology in urban areas. These include more secure, though not invincible, methods of encryption, and wireless carriers throughout the world are upgrading their networks to use these newer technologies.

It is in the context of such growing technical challenges to data collection that intelligence agencies, such as the NSA, have become interested in acquiring cellular encryption keys. "With old-fashioned [2G], there are other ways to work around cellphone security without those keys," says Green, the Johns Hopkins cryptographer. "With newer 3G, 4G and LTE protocols, however, the algorithms aren't as vulnerable, so getting those keys would be essential."

The privacy of all mobile communications — voice calls, text messages and Internet access — depends on an encrypted connection between the cellphone and the wireless carrier's network, using keys stored on the SIM, a tiny chip smaller than a postage stamp, which is inserted into the phone. All mobile communications on the phone depend on the SIM, which stores and guards the encryption keys created by companies like Gemalto. SIM cards can be used to store contacts, text messages, and other important data, like one's phone number. In some countries, SIM cards are used to transfer money. As *The Intercept* reported last year, having the wrong SIM card can make you the target of a drone strike.

SIM cards were not invented to protect individual communications — they were designed to do something much simpler: ensure proper billing and prevent fraud, which was pervasive in the early days of cellphones. Soghoian compares the use of encryption keys on SIM cards to the way Social Security numbers are used today. "Social security numbers were designed in the 1930s to track your contributions to your government pension," he says. "Today they are used as a quasi national identity number, which was never their intended purpose."

Because the SIM card wasn't created with call confidentiality in mind, the manufacturers and wireless carriers don't make a great effort to secure their supply chain. As a result, the SIM card is an extremely vulnerable component of a mobile phone. "I doubt anyone is treating those things very carefully," says Green. "Cell companies probably don't treat them as essential security tokens. They probably just care that nobody is defrauding their networks." The ACLU's Soghoian adds, "These keys are so valuable that it makes sense for intel agencies to go after them."

As a general rule, phone companies do not manufacture SIM cards, nor program them with secret encryption keys. It is cheaper and more efficient for them to outsource this sensitive step in the SIM card production process. They purchase them in bulk with the keys pre-loaded by other corporations. Gemalto is the largest of these SIM "personalization" companies.

After a SIM card is manufactured, the encryption key, known as a "Ki," is burned directly onto the chip. A copy of the key is also given to the cellular provider, allowing its network to recognize an individual's phone. In order for the phone to be able to connect to the wireless carrier's network, the phone — with the help of the SIM — authenticates itself using the Ki that has been programmed onto the SIM. The phone conducts a secret "handshake" that validates that the Ki on the SIM matches the Ki held by the mobile company. Once that happens, the communications between the phone and the network are encrypted. Even if GCHQ or the NSA were to intercept the phone signals as they are transmitted through the air, the intercepted data would be a garbled mess. Decrypting it can be challenging and time-consuming. Stealing the keys, on the other hand, is beautifully simple, from the intelligence agencies' point of view, as the pipeline for producing and distributing SIM cards was never designed to thwart mass surveillance efforts.

One of the creators of the encryption protocol that is widely used today for securing emails, Adi Shamir, famously asserted: "Cryptography is typically bypassed, not penetrated." In other words, it is much easier (and sneakier) to open a locked door when you have the key than it is to break down the door using brute force. While the NSA and GCHQ have substantial resources dedicated to breaking encryption, it is not the only way — and certainly not always the most efficient — to get at the data they want. "NSA has more mathematicians on its payroll than any other entity in the U.S.," says the ACLU's Soghoian. "But the NSA's hackers are way busier than its mathematicians."

GCHQ and the NSA could have taken any number of routes to steal SIM encryption keys and other data. They could have physically broken into a manufacturing plant. They could have broken into a wireless carrier's office. They could have bribed, blackmailed or coerced an employee of the manufacturer or cellphone provider. But all of that comes with substantial risk of exposure. In the case of Gemalto, hackers working for GCHQ remotely penetrated the company's computer network in order to steal the keys in bulk as they were en route to the wireless network providers.

SIM card "personalization" companies like Gemalto ship hundreds of thousands of SIM cards at a time to mobile phone operators across the world. International shipping records obtained by *The Intercept* show that in 2011, Gemalto shipped 450,000 smart cards from its plant in Mexico to Germany's Deutsche Telekom in just one shipment.

In order for the cards to work and for the phones' communications to be secure, Gemalto also needs to provide the mobile company with a file containing the encryption keys for each of the new SIM cards. These master key files could be shipped via FedEx, DHL, UPS or another snail mail provider. More commonly, they could be sent via email or through File Transfer Protocol, FTP, a method of sending files over the Internet.

The moment the master key set is generated by Gemalto or another personalization company, but before it is sent to the wireless carrier, is the most vulnerable moment for interception. "The value of getting them at the point of manufacture is you can presumably get a lot of keys in one go, since SIM chips get made in big batches," says Green, the cryptographer. "SIM cards get made for lots of different carriers in one facility." In Gemalto's case, GCHQ hit the jackpot, as the company manufactures SIMs for hundreds of wireless network providers, including all of the leading U.S.— and many of the largest European — companies.

But obtaining the encryption keys while Gemalto still held them required finding a way into the company's internal systems.

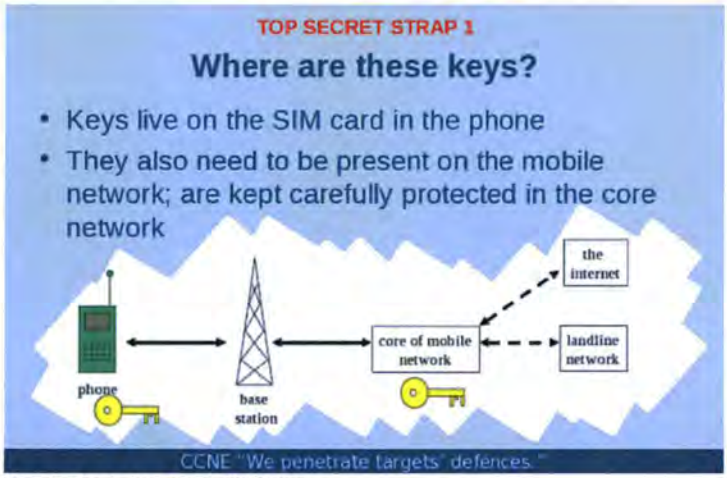


Diagram from a top-secret GCHQ slide.

TOP-SECRET GCHQ documents reveal that the intelligence agencies accessed the email and Facebook accounts of engineers and other employees of major telecom corporations and SIM card manufacturers in an effort to secretly obtain information that could give them access to millions of encryption keys. They did this by utilizing the NSA's X-KEYSCORE program, which allowed them access to private emails hosted by the SIM card and mobile companies' servers, as well as those of major tech corporations, including Yahoo and Google.

In effect, GCHQ clandestinely cyberstalked Gemalto employees, scouring their emails in an effort to find people who may have had access to the company's core networks and Ki-generating systems. The intelligence agency's goal was to find information that would aid in breaching Gemalto's systems, making it possible to steal large quantities of encryption keys. The agency hoped to intercept the files containing the keys as they were transmitted between Gemalto and its wireless network provider customers.

GCHQ operatives identified key individuals and their positions within Gemalto and then dug into their emails. In one instance, GCHQ zeroed in on a Gemalto employee in Thailand who they observed sending PGP-encrypted files, noting that if GCHQ wanted to expand its Gemalto operations, "he would certainly be a good place to start." They did not claim to have decrypted the employee's communications, but noted that the use of PGP could mean the contents were potentially valuable.

The cyberstalking was not limited to Gemalto. GCHQ operatives wrote a script that allowed the agency to mine the private communications of employees of major telecommunications and SIM "personalization" companies for technical terms used in the assigning of secret keys to mobile phone customers. Employees for the SIM card manufacturers and wireless network providers were labeled as "known individuals and operators targeted" in a top-secret GCHQ document.

According to that April 2010 document, "PCS Harvesting at Scale," hackers working for GCHQ focused on "harvesting" massive amounts of individual encryption keys "in transit between mobile network operators and SIM card personalisation centres" like Gemalto. The spies "developed a methodology for intercepting these keys as they are transferred between various network operators and SIM card providers." By that time, GCHQ had developed "an automated technique with the aim of increasing the volume of keys that can be harvested."

The PCS Harvesting document acknowledged that, in searching for information on encryption keys, GCHQ operatives would undoubtedly vacuum up "a large number of unrelated items" from the private communications of targeted employees. "[H]owever an analyst with good knowledge of the operators involved can perform this trawl regularly and spot the transfer of large batches of [keys]."

The document noted that many SIM card manufacturers transferred the encryption keys to wireless network providers "by email or FTP with simple encryption methods that can be broken ... or occasionally with no encryption at all." To get bulk access to encryption keys, all the NSA or GCHQ needed to do was intercept emails or file transfers as they were sent over the Internet — something both agencies already do millions of times per day. A footnote in the 2010 document observed that the use of "strong encryption products ... is becoming increasingly common" in transferring the keys.

In its key harvesting "trial" operations in the first quarter of 2010, GCHQ successfully intercepted keys used by wireless network providers in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan. But, the agency noted, its automated key harvesting system failed to produce results against Pakistani networks, denoted as "priority targets" in the document, despite the fact that GCHQ had a store of Kis from two providers in the country, Mobilink and Telenor. "[I]t is possible that these networks now use more secure methods to transfer Kis," the document concluded.

From December 2009 through March 2010, a month before the Mobile Handset Exploitation Team was formed, GCHQ conducted a number of trials aimed at extracting encryption keys and other personalized data for individual phones. In one two-week period, they accessed the emails of 130 people associated with wireless network providers or SIM card manufacturing and personalization. This operation produced nearly 8,000 keys matched to specific phones in 10 countries. In another two-week period, by mining just six email

addresses, they produced 85,000 keys. At one point in March 2010, GCHQ intercepted nearly 100,000 keys for mobile phone users in Somalia. By June, they'd compiled 300,000. "Somali providers are not on GCHQ's list of interest," the document noted. "[H]owever, this was usefully shared with NSA."

The GCHQ documents only contain statistics for three months of encryption key theft in 2010. During this period, millions of keys were harvested. The documents stated explicitly that GCHQ had already created a constantly evolving automated process for bulk harvesting of keys. They describe active operations targeting Gemalto's personalization centers across the globe, as well as other major SIM card manufacturers and the private communications of their employees.

A top-secret NSA document asserted that, as of 2009, the U.S. spy agency already had the capacity to process between 12 and 22 million keys per second for later use against surveillance targets. In the future, the agency predicted, it would be capable of processing more than 50 million per second. The document did not state how many keys were actually processed, just that the NSA had the technology to perform such swift, bulk operations. It is impossible to know how many keys have been stolen by the NSA and GCHQ to date, but, even using conservative math, the numbers are likely staggering.

GCHQ assigned "scores" to more than 150 individual email addresses based on how often the users mentioned certain technical terms, and then intensified the mining of those individuals' accounts based on priority. The highest-scoring email address was that of an employee of Chinese tech giant Huawei, which the U.S. has repeatedly accused of collaborating with Chinese intelligence. In all, GCHQ harvested the emails of employees of hardware companies that manufacture phones, such as Ericsson and Nokia; operators of mobile networks, such as MTN Irancell and Belgacom; SIM card providers, such as Bluefish and Gemalto; and employees of targeted companies who used email providers, such as Yahoo and Google. During the three-month trial, the largest number of email addresses harvested were those belonging to Huawei employees, followed by MTN Irancell. The third largest class of emails harvested in the trial were private Gmail accounts, presumably belonging to employees at targeted companies.

> ***"PEOPLE WERE SPECIFICALLY HUNTED AND TARGETED BY INTELLIGENCE AGENCIES, NOT BECAUSE THEY DID ANYTHING WRONG, BUT BECAUSE THEY COULD BE USED."***

The GCHQ program targeting Gemalto was called DAPINO GAMMA. In 2011, GCHQ launched operation HIGHLAND FLING to mine the email accounts of Gemalto employees in France and Poland. A top-secret document on the operation stated that one of the aims was "getting into French HQ" of Gemalto "to get in to core data repositories." France, home to one of Gemalto's global headquarters, is the nerve center of the company's worldwide operations. Another goal was to intercept private communications of employees in Poland that "could lead to penetration into one or more personalisation centers" — the factories where the encryption keys are burned onto SIM cards.

As part of these operations, GCHQ operatives acquired the usernames and passwords for Facebook accounts of Gemalto targets. An internal top-secret GCHQ wiki on the program from May 2011 indicated that GCHQ was in the process of "targeting" more than a dozen Gemalto facilities across the globe, including in Germany, Mexico, Brazil, Canada, China, India, Italy, Russia, Sweden, Spain, Japan and Singapore.

The document also stated that GCHQ was preparing similar key theft operations against one of Gemalto's competitors, Germany-based SIM card giant Giesecke and Devrient.

On January 17, 2014, President Barack Obama gave a major address on the NSA spying scandal. "The bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security and that we take their privacy concerns into account in our policies and procedures," he said.

The monitoring of the lawful communications of employees of major international corporations shows that such statements by Obama, other U.S. officials and British leaders — that they only intercept and monitor the communications of known or suspected criminals or terrorists — were untrue. "The NSA and GCHQ view the private communications of people who work for these companies as fair game," says the ACLU's Soghoian. "These people were specifically hunted and targeted by intelligence agencies, not because they did anything wrong, but because they could be used as a means to an end."

ıg service identified. apparently used by gemalto employees- maybe just as teste

s a Gemalto Technical Consultant in Prague. Searching in UDAQ revealed an item in
a.com to a number of @gemalto.com email addresses, including [redacted] and [redacted]
ech Consultant). Investigation on the internet revealed that Yuuwaa (www.yuuwaa.com)
sold by Gemalto. It consists of a USB stick and associated
des access to online storage using a subscription model. It claims to use 128-bit SSL
ge location. The device is aimed at the general consumer market, so presumably Gemalto
usingly, the quotes from "customers" on the website all appear to be from Gemalto

Singapore. His job title is "Sales – Telecom Solutions and Services". He will shortly
with Gemalto)

Device – Product Marketing Manager" at La Ciotat (France). He appears to be some sort
ot seen any indication that he will have any data of interest, so he is unlikely to be worth

METNA-Telecom" and is based in Dubai (from previous knowledge). We did not see
nce we have good coverage of the Dubai office, further investigation is probably

tware/Cloud Computing Innovation WG Chairman" and is not likely to be of interest.

ddle East) and is based in Dubai (see [redacted])

ager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in
nterested in this area, he would certainly be a good place to start.

who was already known about) did not have any useful information or any details of

[redacted] contacts) under OP HIGHLAND FLING.

ion will be useful in future efforts against Gemalto.

THERE ARE TWO basic types of electronic or digital surveillance: passive and active. All intelligence agencies engage in extensive passive surveillance, which means they collect bulk data by intercepting communications sent over fiber-optic cables, radio waves or wireless devices.

Intelligence agencies place high-power antennas, known as "spy nests," on the top of their countries' embassies and consulates, which are capable of vacuuming up data sent to or from mobile phones in the surrounding area. The joint NSA/CIA Special Collection Service is the lead entity that installs and mans these nests for the United States. An embassy situated near a parliament or government agency could easily intercept the phone calls and data transfers of the mobile phones used by foreign government officials. The U.S. embassy in Berlin, for instance, is located a stone's throw from the Bundestag. But if the wireless carriers are using stronger encryption, which is built into modern 3G, 4G and LTE networks, then intercepted calls and other data would be more difficult to crack, particularly in bulk. If the intelligence agency wants to actually listen to or read what is being transmitted, they would need to decrypt the encrypted data.

Active surveillance is another option. This would require government agencies to "jam" a 3G or 4G network, forcing nearby phones onto 2G. Once forced down to the less secure 2G technology, the phone can be tricked into connecting to a fake cell tower operated by an intelligence agency. This method of surveillance, though effective, is risky, as it leaves a digital trace that counter-surveillance experts from foreign governments could detect.

Stealing the Kis solves all of these problems. This way, intelligence agencies can safely engage in passive, bulk surveillance without having to decrypt data and without leaving any trace whatsoever.

"Key theft enables the bulk, low-risk surveillance of encrypted communications," the ACLU's Soghoian says. "Agencies can collect all the communications and then look through them later. With the keys, they can decrypt whatever they want, whenever they want. It's like a time machine, enabling the surveillance of communications that occurred before someone was even a target."

Neither the NSA nor GCHQ would comment specifically on the key theft operations. In the past, they have argued more broadly that breaking encryption is a necessary part of tracking terrorists and other criminals. "It is longstanding policy that we do not comment on intelligence matters," a GCHQ official stated in an email, adding that the agency's work is conducted within a "strict legal and policy framework" that ensures its activities are "authorized, necessary and proportionate," with proper oversight, which is the standard response the agency has provided for previous stories published by *The Intercept*. The agency also said, "[T]he UK's interception regime is entirely compatible with the European Convention on Human Rights." The NSA declined to offer any comment.

It is unlikely that GCHQ's pronouncement about the legality of its operations will be universally embraced in Europe. "It is governments massively engaging in illegal activities," says Sophie in't Veld, a Dutch member of the European Parliament. "If you are not a government and you are a student doing this, you will end up in jail for 30 years." Veld, who chaired the European Parliament's recent inquiry into mass surveillance exposed by Snowden, told *The Intercept*: "The secret services are just behaving like cowboys. Governments are behaving like cowboys and nobody is holding them to account."

The Intercept's Laura Poitras has previously reported that in 2013 Australia's signals intelligence agency, a close partner of the NSA, stole some 1.8 million encryption keys from an Indonesian wireless carrier.

A few years ago, the FBI reportedly dismantled several transmitters set up by foreign intelligence agencies around the Washington, D.C. area, which could be used to intercept cellphone communications. Russia, China, Israel and other nations use similar technology as the NSA across the world. If those governments had the encryption keys for major U.S. cellphone companies' customers, such as those manufactured by Gemalto, mass snooping would be simple. "It would mean that with a few antennas placed around Washington, D.C., the Chinese or Russian governments could sweep up and decrypt the communications of members of Congress, U.S. agency heads, reporters, lobbyists and everyone else involved in the policymaking process and decrypt their telephone conversations," says Soghoian.

"Put a device in front of the U.N., record every bit you see going over the air. Steal some keys, you have all those conversations," says Green, the Johns Hopkins cryptographer. And it's not just spy agencies that would benefit from stealing encryption keys. "I can only imagine how much money you could make if you had access to the calls made around Wall Street," he adds.

GCHQ slide.

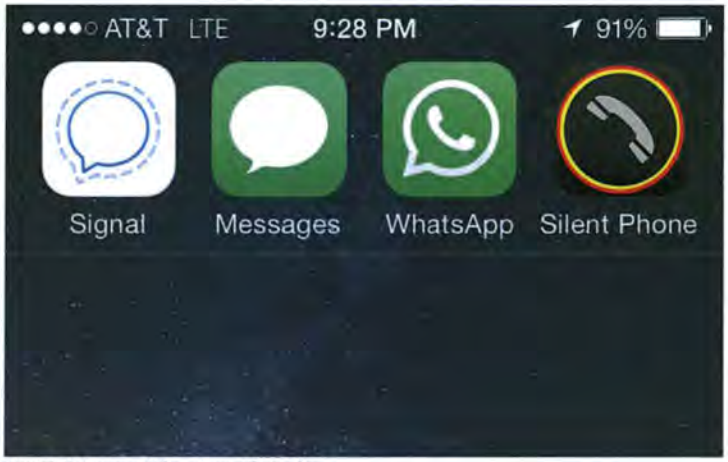
THE BREACH OF Gemalto's computer network by GCHQ has far-reaching global implications. The company, which brought in $2.7 billion in revenue in 2013, is a global leader in digital security, producing banking cards, mobile payment systems, two-factor authentication devices used for online security, hardware tokens used for securing buildings and offices, electronic passports and identification cards. It provides chips to Vodafone in Europe and France's Orange, as well as EE, a joint venture in the U.K. between France Telecom and Deutsche Telekom. Royal KPN, the largest Dutch wireless network provider, also uses Gemalto technology.

In Asia, Gemalto's chips are used by China Unicom, Japan's NTT and Taiwan's Chungwa Telecom, as well as scores of wireless network providers throughout Africa and the Middle East. The company's security technology is used by more than 3,000 financial institutions and 80 government organizations. Among its clients are Visa, Mastercard, American Express, JP Morgan Chase and Barclays. It also provides chips for use in luxury cars, including those made by Audi and BMW.

In 2012, Gemalto won a sizable contract, worth $175 million, from the U.S. government to produce the covers for electronic U.S. passports, which contain chips and antennas that can be used to better authenticate travelers. As part of its contract, Gemalto provides the personalization and software for the microchips implanted in the passports. The U.S. represents Gemalto's single largest market,

accounting for some 15 percent of its total business. This raises the question of whether GCHQ, which was able to bypass encryption on mobile networks, has the ability to access private data protected by other Gemalto products created for banks and governments.

As smart phones become smarter, they are increasingly replacing credit cards and cash as a means of paying for goods and services. When Verizon, AT&T and T-Mobile formed an alliance in 2010 to jointly build an electronic pay system to challenge Google Wallet and Apple Pay, they purchased Gemalto's technology for their program, known as Softcard. (Until July 2014, it previously went by the unfortunate name of "ISIS Mobile Wallet.") Whether data relating to that, and other Gemalto security products, has been compromised by GCHQ and the NSA is unclear. Both intelligence agencies declined to answer any specific questions for this story.



Signal, iMessage, WhatsApp, Silent Phone.

PRIVACY ADVOCATES and security experts say it would take billions of dollars, significant political pressure, and several years to fix the fundamental security flaws in the current mobile phone system that NSA, GCHQ and other intelligence agencies regularly exploit.

A current gaping hole in the protection of mobile communications is that cellphones and wireless network providers do not support the use of Perfect Forward Secrecy (PFS), a form of encryption designed to limit the damage caused by theft or disclosure of encryption keys. PFS, which is now built into modern web browsers and used by sites like Google and Twitter, works by generating unique encryption keys for each communication or message, which are then discarded. Rather than using the same encryption key to protect years' worth of data, as the permanent Kis on SIM cards can, a new key might be generated each minute, hour or day, and then promptly destroyed. Because cellphone communications do not utilize PFS, if an intelligence agency has been "passively" intercepting someone's communications for a year and later acquires the permanent encryption key, it can go back and decrypt all of those communications. If mobile phone networks were using PFS, that would not be possible — even if the permanent keys were later stolen.

The only effective way for individuals to protect themselves from Ki theft-enabled surveillance is to use secure communications software, rather than relying on SIM card-based security. Secure software includes email and other apps that use Transport Layer Security (TLS), the mechanism underlying the secure HTTPS web protocol. The email clients included with Android phones and iPhones support TLS, as do large email providers like Yahoo and Google.

Apps like TextSecure and Silent Text are secure alternatives to SMS messages, while Signal, RedPhone and Silent Phone encrypt voice calls. Governments still may be able to intercept communications, but reading or listening to them would require hacking a specific handset, obtaining internal data from an email provider, or installing a bug in a room to record the conversations.

"We need to stop assuming that the phone companies will provide us with a secure method of making calls or exchanging text messages," says Soghoian.

———

Documents published with this article:

- CNE Access to Core Mobile Networks
- Where Are These Keys?
- CCNE Successes Jan10-Mar10 Trial
- DAPINO GAMMA CNE Presence Wiki
- DAPINO GAMMA Gemalto Yuaawaa Wiki
- DAPINO GAMMA Target Personalisation Centres Gemalto Wiki
- IMSIs Identified with Ki Data for Network Providers Jan10-Mar10 Trial
- CCNE Stats Summaries Jan10-Mar10 Trial
- CCNE Email Harvesting Jan10-Mar10 Trial
- CCNE Email Addresses Jan10-Mar10 Trial
- PCS Harvesting at Scale

Additional reporting by Andrew Fishman and Ryan Gallagher. Sheelagh McNeill, Morgan Marquis-Boire, Alleen Brown, Margot Williams, Ryan Devereaux and Andrea Jones contributed to this story. Erin O'Rourke provided additional assistance.

Top photo: Shutterstock

✉ Email the authors: jeremy.scahill@theintercept.com, josh.begley@theintercept.com

RECOMMENDED

Prosecutor Says Tsarnaev was "Holy Warrior"

The "Snowden is Ready to Come Home!" Story: a Case Study in Typical Media Deceit

Feds: Ferguson Preys Viciously on Black Residents

Petraeus Plea Deal Reveals Two-Tier Justice System for Leaks

New Zealand Spies on Neighbors in Secret 'Five Eyes' Global Surveillance

Top Lobbyist: 2016 To Be "Bumper Year" Thanks to Clinton Campaign

The Tsarnaev Trial and the Blind Spots in 'Countering Violent Extremism'

Benjamin Netanyahu's Long History of Crying Wolf About Iran's Nuclear Weapons

The Washington Post

The Switch

Obama said everyone wants secure mobile communications. But the NSA worked to undermine that.

By Andrea Peterson February 20

Just a week ago, President Obama assured the public that he understood the importance of securing the privacy of mobile phone networks.

"Ultimately, everybody — and certainly this is true for me and my family — we all want to know that if we're using a smartphone for transactions, sending messages, having private conversations, that we don't have a bunch of people compromising that process," Obama told technology site re/code in an interview. "So there's no scenario in which we don't want really strong encryption."

But a new report published by the Intercept alleges that British and American spies actively sought to undermine the security features that protect mobile networks around the world.

A team of operatives from the National Security Agency and its British equivalent, GCHQ, hacked into a Dutch company that makes SIM cards to obtain encryption keys that are used to protect the cellphone communications of millions of people around the world in 2010, according to the Intercept's story, which is based on documents from former

NSA contractor Edward Snowden. Stealing those encryption keys essentially makes it much easier for the spy agencies to eavesdrop on communications that would have otherwise been protected.

"That can't be squared" with the president's stated desire for those communications to be secure, according to Matthew Green, a cryptography expert and professor at the Johns Hopkins Information Security Institute.

Some privacy advocates have raised concerns that Obama's rhetoric may indicate he is not aware of some government surveillance activities. "I suspect the president was not fully briefed on the extent law enforcement and intelligence agencies develop, acquire and exploit vulnerabilities in the software we all use," said Christopher Soghoian, principal technologist for the American Civil Liberties Union's Speech, Privacy and Technology Project. "Otherwise, I don't know how he could say that with a straight face."

The White House declined to comment for this story. The NSA did not immediately respond to a request for comment.

Even if the government did not target the encryption keys for domestic use, what it was doing, Green said, did fundamentally compromise the security of mobile phone networks globally.

It's worth noting that the Intercept's report suggests some of the practices of the company, Gemalto, may have also put the encryption keys at added risk in the first place — like occasionally transferring them to mobile network operators unencrypted. And it is the NSA's job to collect signals for foreign intelligence purposes. The agency needs a warrant to target an American's calls or e-mails, but generally does not require the same standards for targeting foreigners when collecting overseas.

But in the wake of the Snowden revelations, Obama has said the United States respects

the privacy of ordinary people regardless of their nationality. "The bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security and that we take their privacy concerns into account in our policies and procedures," he said during a speech on the spying last January.

However, the Intercept's report indicates that the GCHQ used the NSA's X-KEYSCORE program to access the private communications of Gemalto employees in an attempt to gain access to information about the SIM card encryption keys.

This isn't the first time concerns have been raised about a perceived disconnect between Obama's statements on digital security and government actions or policy proposals. Technical experts say the stories he uses to illustrate the risks of tech companies' encryption expansions and calls from senior administration officials for the companies to maintain ways for law enforcement to access data are at odds with how the technology actually works. The president ultimately did not take a side on the larger encryption issue during the re/code interview — instead, saying there needs to be a "public debate."

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government.